REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
13 June 2012	Master's Thesis	25 July 2011 - 17 June 2012

4. TITLE AND SUBTITLE

Deterrence in Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Matthew Rivera, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton BLVD.
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

There are significant differences between nuclear attack and cyber-attack, but the development of cyber deterrence policy is relevant to the total defense of the United States' critical infrastructure and networked cyber systems. The rapidity, ambiguity of origination, and inexpensiveness of a cyber-attack creates a different problem not easily addressed by the strategies used in the implementation of nuclear deterrence. Similar to the nuclear deterrence policy developed during the Cold War, a policy for deterrence to compliment the United States' defense of its interests in cyberspace from nefarious acts is needed today. Influencing the mental calculus of a potential adversary to dissuade them from conduct that threatens the United States is a critical aspect of defending the nation's interests in cyberspace.

Having the capabilities in cyberspace to effectively respond to enemy aggression is critical to deterrence as a strategy to defend the nation's critical infrastructure. The cyber-attacks conducted against Georgia and Estonia during their conflicts with Russia demonstrates the ability for widespread effects at very little cost. While the private sector must do more to ensure critical

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
Unclassified	Unclassified	Unclassified	Unclassified Unlimited	79	757-443-6301

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

DETERRENCE IN CYBERSPACE

by

Matthew Rivera

Lieutenant Commander, United States Navy

DETERRENCE IN CYBERSPACE

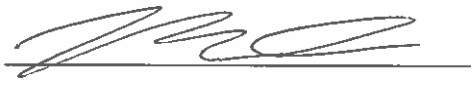
by

Matthew Rivera

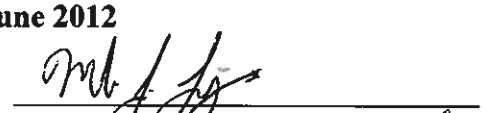
Lieutenant Commander, United States Navy

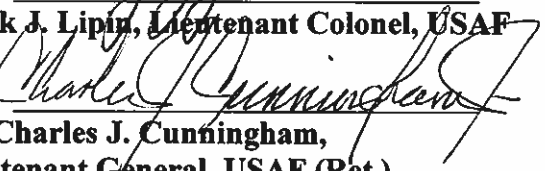
A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

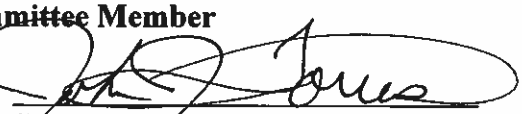
This paper is entirely my own work except as documented in footnotes.

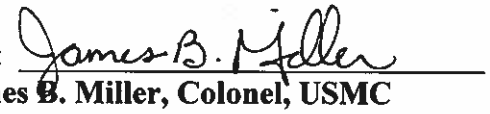
Signature: 

13 June 2012

Thesis Adviser: Signature: 
Mark J. Lipin, Lieutenant Colonel, USAF

Approved by: Signature: 
Dr. Charles J. Cunningham,
Lieutenant General, USAF (Ret.)
Committee Member

Signature: 
John J. Torres, Colonel, USAF
Committee Member

Signature: 
James B. Miller, Colonel, USMC
Director, Joint Advanced Warfighting School

ABSTRACT

There are significant differences between nuclear attack and cyber-attack, but the development of cyber deterrence policy is relevant to the total defense of the United States' critical infrastructure and networked cyber systems. The rapidity, ambiguity of origination, and inexpensiveness of a cyber-attack creates a different problem not easily addressed by the strategies used in the implementation of nuclear deterrence. Similar to the nuclear deterrence policy developed during the Cold War, a policy for deterrence to compliment the United States' defense of its interests in cyberspace from nefarious acts is needed today. Influencing the mental calculus of a potential adversary to dissuade them from conduct that threatens the United States is a critical aspect of defending the nation's interests in cyberspace.

Having the capabilities in cyberspace to effectively respond to enemy aggression is critical to deterrence as a strategy to defend the nation's critical infrastructure. The cyber-attacks conducted against Georgia and Estonia during their conflicts with Russia demonstrates the ability for widespread effects at very little cost. While the private sector must do more to ensure critical infrastructures are adequately protected, the government similarly needs to better develop policies and associated consequences to deter cyber-attacks. The aspects of nuclear deterrence considered relevant to cyber deterrence in this paper are attribution, penalty, credibility, definition of attack, dependency, counter-productivity, awareness, and futility.

Table of Contents

INTRODUCTION 1
CHAPTER 1: ASPECTS OF DETERRENCE 6
Overview 6
Awareness 7
Attribution 8
Penalty 9
Credibility 10
Attack Definition 10
Dependency 12
Counter-Productivity 13
Futility 13
Summary 14
CHAPTER 2: POLICIES AND DIRECTIVES 16
Overview 16
Executive Directives, National Strategies, and Departmental Directives 16
Executive 17
The National Security Strategy of the United States of America 17
Executive Order 13231 - Critical Infrastructure Protection in the Information Age 18
National Strategy for Homeland Security 19
Cyberspace Policy Review 20
Comprehensive National Cybersecurity Initiative 21
Homeland Security Presidential Directive 7 22
National Strategy for the Physical Protection of CI and Key Assets 23
Department of Defense 24
The National Military Strategy of the United States of America 24
Strategy for Homeland Defense and Civil Support 25
DoD Policy and Responsibilities for Critical Infrastructure Directive 3020.40 26
Defense Industrial Base: Critical Infrastructure and Key Resources SSP 26
Department of Defense Strategy for Operating in Cyberspace 27
Department of Homeland Security 29
National Strategy to Secure Cyberspace 29
National Infrastructure Protection Plan 30

Summary 31
CHAPTER 3: CYBER-ATTACK 33
Overview 33
Stuxnet - Background 33
From Worm to Cyber-Weapon 35
Discovery 36
Aspects of Deterrence Applied 36
Stuxnet Summary 37
Cyberspace: An Insurgency Force Multiplier 38
Civilian Mass Mobilization 39
Exchange of Communication 39
Redefining the Battlefield 41
Aspects of Deterrence Applied 42
Summary of Cyberspace: An Insurgency Force Multiplier 42
Estonia and Georgia - Background 43
Estonia's and Georgia's Cyberspace Dependency 44
Cyber-attacks against Estonia and Georgia 45
Aspects of Deterrence Applied 46
Summary of Estonia and Georgia 47
Why Seek Deterrence in Cyberspace 47
Critical United States Infrastructures Susceptible to Cyber-attack 49
Water Supplies 50
Power Grid 50
Rail and Air Traffic Control 51
Summary 52
CHAPTER 4: RECOMMENDATIONS 54
CONCLUSION 58
Appendix 1 – National Policy versus Cyber Deterrence 61
BIBLIOGRAPHY 63
VITA 69

Figure 3-1 - How Stuxnet Propagates 34

INTRODUCTION

This thesis will show that, similar to the nuclear deterrence policy developed during the Cold War, a policy for deterrence to compliment the United States' defense of its interests in cyberspace from nefarious acts is needed today. By defining areas where deterrence can be applied, analyzing current policy toward cyber defense, and examining real world cyber-attacks to frame the battle space the author will make recommendations to better address the needs of a policy of deterrence in cyberspace. The overall framework for this discussion deterrence in cyberspace is an author created tool found in Appendix 1.

A policy in cyber deterrence that contributes to influencing the mental calculus of potential adversaries to dissuade them from conduct that threatens the United States is a critical aspect of defending the nation's interests in cyberspace. The chart titled National Policy Shortfalls Tool found in Appendix 1 - National Policy versus Cyber Deterrence will be used to examine the differences between a set of characteristics of cyber deterrence defined in Chapter 1 and compare them to current policy documents discussed in Chapter 2.

Chapter 1, in the author's view, identifies and defines the aspects of nuclear deterrence considered relevant to cyber deterrence in this paper, which are: attribution, penalty, credibility, definition of attack, dependency, counter-productivity, awareness, and futility. These aspects of deterrence will be applied to policy documents to determine where emphasis needs to be placed in order to fully develop a cyber deterrence policy. Also, this paper will use the eight defined aspects of deterrence applied to cyberspace to analyze known examples of cyber-attack (e.g. Stuxnet virus) that will be covered in Chapter 3, and what measures could have been taken to deter. Once the aspects of deterrence are developed in Chapter 1, they will be used to provide a

baseline (x-axis) with which to compare current policies and directives (y-axis) to show areas that still require further development and study.

In Chapter 2 the policies and directives used to define the roles and responsibilities, as well as approach to the defense of cyberspace, will be compared to the aspects of deterrence defined in Chapter 1. There are significant differences between nuclear attack and cyber-attack, but the development of cyber deterrence policy is relevant to the total defense of the United States' critical infrastructure and networked cyber systems. The rapidity, ambiguity of origination, and inexpensiveness of a cyber-attack creates a different problem not easily addressed by the strategies used in the implementation of nuclear deterrence.[1] The threat of escalated retaliation from a nuclear attack, or the inability to completely render the attacked incapable of retaliation was an important aspect on which the Mutually Assured Destruction policy of nuclear deterrence depended. In cyberspace the current susceptibility of the nation's critical infrastructure coupled with the likelihood an attacker can cause vast amounts of damage with little concern for being identified removes the threat of retaliation. Even as the United States continues to identify and limit avenues for cyber exploitation of its critical infrastructure, other nations are subject to similar vulnerabilities and must consider the repercussions from initiating nefarious cyber activities knowingly or unknowingly.

Chapter 3 explores why the requirements for a policy of deterrence in cyberspace is an important aspect to cyber defense. Having the capabilities in cyberspace to effectively respond to enemy aggression is as critical to deterrence as is a strategy to defend the nation's critical infrastructure. The cyber-attacks conducted against Georgia and Estonia during their conflicts with Russia demonstrates the ability for widespread effects at very little cost. There are several areas that are currently susceptible and attractive to the adversary to carrying out a cyber-attack.

[1] Martin C. Libiciki, *Cyberdeterrence and Cyberwar*, (Santa Monica: RAND, 2009), 18.

Susceptible to cyber-attack due to the level of protection currently afforded are the private industries that manage the nation's water supplies, power grids, and air and rail traffic control systems. These are attractive to an attacker for the large scale devastation that could be achieved with very few resources being committed. The majority of the United States' national policy documents recognize the importance of cooperation between the private sector and government in the protection of the nation's critical infrastructure. While the private sector must do more to ensure critical infrastructures are adequately protected, the government similarly needs to better develop policies and associated consequences to deter cyber-attacks.[2]

Large scale attacks against the United States' cyber connected infrastructure are unlikely to come from a peer or near-peer competitor during a peace time environment due in large part to the interdependence of those systems. What affects one nation may inevitably affect another in today's globally connected societies. However, during the conduct of an open conflict between those same nations, reluctant to attack during times of peace, an overt attack is more likely because the laws and policies available to prosecute cyber related crime are still developing and ramifications of attacks are not always fully understood, or immediately recognized, as was the case of the Stuxnet virus that will be introduced in Chapter 3. The threat of cyber espionage is the area of focus that is necessary in the absence of war with other nations. Defensive capabilities, policies, and procedures are the most effective means to prevent this type of attack.[3] The United States must also continue to develop its ability to not only defend the nation's critical infrastructure and networks in cyberspace, but also to expand cyber offensive capabilities that are just as covert as those that would attack.

---

[2] U.S. President, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* (Washington, DC: Government Printing Office, February 2003), 20.

[3] 112th Cong., 1st sess, *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology,* (Washington, DC: Government Printing Office, 2011), 36.

There are areas where a policy of deterrence may seem largely ineffective and must be approached by different means. The use of cyberspace as a force multiplier, or a flattening of the battlefield, is a growing concern for the tactical commander on the ground. As seen over the last decade of conflict in Iraq and Afghanistan, the ability to mobilize and coordinate forces enabled through the use of cell phones, websites, and other cyber capabilities has allowed a largely inferior force to effectively stifle a more technological and proven force on the conventional field of battle. Communicating target information, areas of operations, and reframing an operational failure into a strategic success by the insurgents was not as possible in near real time during previous conflicts as it is now.

Deterrence alone will not prevent the progression of cyber-attacks. Indeed, a combination of laws tailored to cyber-crime, international agreements – treaties, laws, or policies that are coordinated to prevent cyber-crime – improved forensics, and other strategies are required to prevent future cyber-attacks. Concurrently, establishing policy that relies solely on the defense of cyberspace will continue to invite attack, and maintain the United States as a reactionary participant vice a true power in the cyber realm. A multi-pronged approach will be necessary to deter those individuals not representing any particular organization and allow for conventional actions, including computer network attacks (CNA) and computer network exploitation (CNE), to be legitimized when a serious threat is identified.

Because cyberspace is a manmade construct, the notion that an impenetrable barrier to attack can ever be constructed is difficult. Studies show that the industry average is about 15-50 errors per 1000 lines delivered code.[4] Almost all systems most likely have vulnerabilities that are susceptible to infiltration and often can be manipulated by an attacker long before the defenders are even aware the system was affected in a nefarious way. Even those systems not

[4] Steve McDonnell, *Code Complete*, (Redmond: Microsoft Press, 2004), 176.

connected in some way to the global network are not immune from attack. In 2010, the Natanz nuclear facility in Iran was targeted through the use of a computer virus designed to target Siemens industrial software and cripple Iran's ability to operate nuclear centrifuges designed to enrich uranium used to produce nuclear weaponry.[5] Due to the similarities in control networks used in the United States, there are similar susceptibilities in critical national infrastructure.[6]

[5] Yossi Melman, "Computer virus in Iran actually targeted larger nuclear facility," Haaretz.com. http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052 (accessed November 11, 2011).

[6] Megha Rajagopalan, "Remember Stuxnet? Why the U.S. is Still Vulnerable," Pro Republica.com http://www.propublica.org/article/remember-stuxnet-why-the-u.s.-is-still-vulnerable (accessed May 18, 2012).

CHAPTER 1: ASPECTS OF DETERRENCE

Overview

> Deterrence is the art of producing, in the mind of the enemy, the fear to attack! …the whole point of a Doomsday machine is lost if you keep it a secret![1]

Deterrence is the inhibition of criminal behavior by fear especially of punishment, or the maintenance of military power for the purpose of discouraging attack, as defined by Merriam-Webster's dictionary.[2] The two types of deterrence are general deterrence and specific deterrence. General deterrence is designed to establish a set of laws and methods of enforcement that will dissuade any actor from engaging in disruptive behavior.[3] This approach attempts to prevent or reduce the likelihood that such behavior will manifest itself in the general population. Attempting to affect an individual's rational decision making process to ensure future behavior is within the established boundaries. Specific deterrence focuses on targeting known offenders of a general deterrence strategy to prevent a reoccurrence of the original infraction.[4] Fundamental to this approach is the notion that the motivation that caused a violation of the original boundaries can be curtailed if a tailored punishment can be exacted. For either strategy of deterrence to have an appreciable effect there are aspects that must be tied to the definition: attribution – the identification of the aggressor directly or indirectly responsible for the attack; penalty – ensuring the imposed punishment sufficiently raises the cost-benefit analysis of the adversary; credibility – the penalty imposed is generally accepted as reasonable to the damage done as a result of an

---

[1] Peter Sellers, *Dr. Strangelove Or: How I Learned to Stop Worrying and Love the Bomb*, DVD, directed by Stanley Kubrick (Los Angles: Turner Classic Movies, 1964).

[2] Merriam-Webster, "Deterrence," Merriam-Webster, http://www.merriam-webster.com/dictionary/deterrence (accessed May 24, 2012).

[3] K. A. Taipale, "Cyber-Deterrence," in *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization*, ed. Pauline C. Reich. (Hershey: IGI Global, 2009), 14.

[4] Ibid.

attempt or successful attack; definition of attack – there are various ways to conduct a cyber-attack (e.g. data disruption, espionage, destruction), which are those attacks that a policy of deterrence should address; dependency – when an aggressor believes or is in fact itself dependent on, or benefits from the same system that is to be attacked; counter-productivity – an attack carried out that would undermine an aggressor's larger interest; awareness – nuclear attack is obvious, but there is the possibility that an attack in cyber space can go unnoticed; and, futility – the idea that the result of an attack can be overcome by either resiliency or redundancy of capabilities. These aspects are used to define the x-axis of Table 1 - National Policy Shortfalls Tool to draw a comparison between current policy documents concerning cyberspace. An examination of each aspect as it applies to the theory of deterrence will develop a better understanding of how cyber-attackers can be dissuaded. Not included in the discussion is the aspect of accountability which is covered by attribution and penalty.

Deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability actually to achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort.[5]

Awareness

For any strategy in deterrence to succeed the potential perpetrator must be made aware that a retaliatory strike is likely to occur and the capability exists to carry out the strike. While the actual form need not be made obvious, and probably should not be to allow for some flexibility, an attacker's ignorance of a retaliatory strike could lead to an attack that may have otherwise been prevented. Richard Clarke writes,

[5] William Kaufmann, *The Evolution of Deterrence 1945–1958*, (Pittsburgh: RAND, 1958), 79.

> A public declaration of about what we would do in case of a cyber-attack should, however, not limit future decisions. There needs to be a certain 'constructive ambiguity' in what is said. In the event of a major cyber-attack, there will likely be an unhelpful ambiguity about who attacked us, and our declaratory policy needs to take that into account as well.[6]

Therefore, developing a policy that does not exclude future cyber-attacks not already imagined and then articulating that policy to the public re-enforces a strategy in deterrence. Once a deterrence policy is developed, it must be communicated and continuously evaluated to address the ever changing nature of cyberspace and how cyberspace can be maliciously employed.

Attribution

With conventional attacks, the forensics for identifying a perpetrator are well developed and are well understood enabling an appropriate punishment to be enforced. For someone to commit a physical crime and cleverly disguise their involvement can be relatively difficult compared to the ease in which the source of a cyber-attack can be confused. Increasing the chance of being caught can dissuade an individual or organization from conducting an attack and the potential for deterrence is achieved. If there is a high probability that an attack will go unrecognized allowing for an escape or that the ability to trace its origins, then the probability of an attack increases.[7] This can be seen in the tactics employed by the insurgents in Iraq and Afghanistan in the use of improvised explosive devices. The insurgents are able to either remotely detonate or set to trigger from an event, such as a vehicle passing by, and escape the area with little threat to them personally.

[6] Richard A. Clarke, *Cyberwar*, (New York: HarperCollins, 2010), 13.

[7] K. A. Taipale, "Cyber-Deterrence," in *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization*, ed. Pauline C. Reich. (Hershey: IGI Global, 2009), 32.

However, due to the forensics currently associated with the detection and attribution of cyber-attacks, the threshold for attribution will largely be one tried in the court of public opinion and need not be proven beyond a reasonable doubt.[8] The level of destructiveness of the original attack, degree of criticism the United States is willing to tolerate, and benefits gained from a counter attack should be the determinant in its execution. Policies designed that sufficiently restrict the ability to counterattack based on insufficient evidence will undermine the legitimacy of a strategy of deterrence.

Penalty

This approach has dominated the landscape of deterrent strategies. This concept focuses on developing a known set of consequences in an attempt to discourage or prevent an attack from ever occurring. As stated earlier, the United States' position of mutually assured destruction as a nuclear strategy to hold the Soviet Union at bay relies on the retaliation of an attack to be too costly. It is also used in law enforcement to deter individuals from committing a crime knowing the punishment that will be levied against the offender. However, based on the unique characteristics of cyberspace, namely a low probability of detection coupled with the low probability of being identified as the attacker, the risk of being appropriately punished is also minimal. As advances in cyber-forensics and tracking software improve, this may be a viable strategy. Currently attributing, especially across international borders where law enforcement may lack resources to prosecute and United States jurisdiction does extend, can be extremely difficult and time consuming; however, this is improving as other nations become increasingly connected.[9]

[8] Richard A. Clarke, *Cyberwar*, (New York: HarperCollins, 2010), 17.
[9] Ibid., 24.

Credibility

Inherent to the theory of deterrence is that any implied or perceived threat of retaliation will be exercised and is within the capabilities of the organization making the threat. This is one area that is difficult to exercise in cyberspace, because the response must be measured to provide a proportionate punishment to the infraction. Thus, it does not test the will of those charged with carrying out the threat. Determining the appropriate level of retaliation is important in developing a credible policy and will directly impact its enforcement. If the perception is that a threat is too severe and there is a reluctance to enforce it this will limit the future effectiveness of a deterrence policy. When a threat is made and the threshold is crossed invoking the stated punishment there must be an unambiguous response to lend credibility to any future threat against cyber-attacks.

If deterrence fails to prevent an attack, the policies and laws must be enforced and the attacker held accountable. This will be critical in demonstrating that the consequences of disruptive behavior are real and serve to ward off any future attacks and reinforce the credibility associated with the deterrence. Any deviation in enforcement of stated punishments can undermine the intent of a deterrence policy. This highlights the importance of selecting a set of consequences that are comparable in severity to the type of behavior that is sought to be deterred.

Attack Definition

To help develop the policy, cyber-attacks must be categorized to better identify retaliatory responses available. Cyber-attacks are carried out in primarily three forms: cyber-espionage, those generally carried out by state actors; data disruption, attacks designed to target civilian or military information and infrastructure; and cyber isolation, those attacks which

attempt to remove access to cyberspace.[10] These three categories combine to describe the physical effects that a cyber-attack can cause, but does not include any psychological cyber-attack effects that do not represent a threat on a national or strategic level.

Cyber-espionage

Cyber-espionage by nation-state actors has become an increasing threat to national security by the theft of intellectual property. As the United States increases the capability and capacity to detect and identify cyber-espionage attacks, their impact has also become better understood. However, espionage in any form is common among nation-states and imagining a sufficiently high cost-benefit ratio when this activity is ultimately deterred is difficult; "however, these activities are generally more appropriately addressed through other strategies, including cyber-security, law enforcement and diplomacy, rather than through deterrence. But, there may be particularly aggressive forms of exploitation (particularly where activity appears to be probing the domain in preparation for attack) where direct or indirect deterrence strategies may be employed. One of the problems in cyber is that it is difficult to distinguish between exploitation and probe. Response is likely to be highly contingent on circumstances. Thus, activity that might be tolerated during a period of relative political calm might be subject to specific deterrent threats during times of escalating crisis."[11]

Data Disruption

A more significant and destructive form of cyber-attack are those attacks designed to affect data by disruption or manipulation of information systems or infrastructure. These cyber-attacks can offer an adversary a strategic advantage by altering the understanding of the battle

[10] K. A. Taipale, "Cyber-Deterrence," in *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization*, ed. Pauline C. Reich. (Hershey: IGI Global, 2009), 60.
[11] Ibid., 60.

space if directed against intelligence systems, or camouflage specific activities in an effort to achieve surprise before kinetic operations begin. As evidenced by the Stuxnet worm on the Iranian Natanz Nuclear Enrichment Facility this form of cyber-attack can cause catastrophic failure of critical infrastructure systems that are only noticeable after the damage has occurred.[12]

These data disruption types of cyber-attacks, on a large enough scale, can potentially impact the United States national and economic security. Cyber-attacks against critical infrastructure and key assets that compromise the nations' ability to supply electricity, control the movements of aircraft and sea craft, and affect food or water supplies are strategic and the target of a policy statement on cyber deterrence.

Cyber-isolation

The third category of cyber-attack is that of cyber-isolation. Generally these types of cyber-attacks are of the Distributed Denial of Service (DDoS) which removes access to websites. These types of attacks, when limited in duration, are more of a nuisance and not a strategic threat to the United States' national security; however, an attack that occurs over an extended time period and prevents access to critical parts of either service or economic infrastructures could be strategic and is required to be a part of cyber deterrence.

Dependency

This approach highlights the global connectedness of today's countries, both allies and adversaries. There is little incentive on the part of a would be attacker to disrupting or destroying a system or systems that an attacker utilizes. For example, a cyber-attack originating from China on the financial infrastructure of the United States is very unlikely due to "Chinese

[12] Ralph Langner, *Cracking Stuxnet, a 21st-century cyber weapon*, TED, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (accessed May 24, 2012).

government officials -- many of whom, in their private lives, tend to be very wealthy, involved very much in the stock market in the international finance -- they may be reluctant to disrupt the financial network, because they could suffer as much as the United States."[13] This approach may be effective on larger scales of dependency, but may not translate to the smaller organizations or individuals seeking to conduct attacks.

Counter-Productivity

When the potential exists that an attack would undermine the larger interests of an attacker, the associated counter-productivity may sufficiently deter.

> Counter-productivity can be normative, for example, where an attack might be tactically successful but is strategically counterproductive because it undermines the attacker's motivational goals, political or moral legitimacy, or general support. Or, it can be instrumental as well, for example, where it legitimizes a particular tactic—*i.e.*, cyber-attacks—to which the attacker may then itself be exposed.[14]

This may be the case with the example in highlighted in Chapter 3 involving a suspected linkage between a cyber power and the Stuxnet virus.

Futility

This approach to cyber deterrence is not based on the ability to defend against an attack, but rather to demonstrate that even a successful attack, whether discovered immediately or allowed to run its course, has no measurable effect on capabilities. Two areas can be used to illustrate how this tactic may be employed to dissuade an attack.

In the case of distributed denial of service (DDoS) attacks as suffered by Estonia in 2007 and Georgia in 2008 the attack could have been rendered ineffective had there been a reserve

---

[13] James Lewis, "Cyberwar!" Public Broadcasting Service, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html (accessed May 25, 2012)

[14] K. A. Taipale, "Cyber-Deterrence," in *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization*, ed. Pauline C. Reich. (Hershey: IGI Global, 2009), 41.

bandwidth available to absorb the attack. Hackers would have believed they carried out a successful attack, but not met the objectives due to the built in redundancies rendering the attack of little consequence. This capability already exists with most major companies who routinely absorb this magnitude of attack on a daily basis.[15] This may result in an escalation of attackers and bandwidth controllers, but the relative cost of maintaining a reserve of bandwidth compared to the cost of recovery from a DDoS attack makes this an attractive approach for this type of attack.

The other area that can be served by the rendering attacks futile is in the use of duplication. All data contained on computers is easily replicated and would allow for easy recovery in the event of an attack that destroys information on a given system.[16] This can be effective at frustrating attackers by having the ability to quickly, near instantaneously, recover from an attack by maintaining a perfect copy of the original data that can be used as often as necessary to restore corrupted systems.[17]

For this approach to be effective the attackers must be made aware of the system's ability to quickly increase bandwidth or recover from an attack without generating any additional challenge incentive for the attacker.

Summary

This chapter articulated the aspects involved with the theory of deterrence and how penalty, credibility, definition of attack, dependency, counter-productivity, awareness, and futility each individually contribute. The National Policies Shortfall Tool, found in Appendix 1 -

[15] Juan Carlos Perez, "DDoS Attackers Continue Hitting Twitter, Facebook, Google," PC World, http://www.pcworld.com/businesscenter/article/169893/ddos_attackers_continue_hitting_twitter_facebook_google.html (accessed October 13, 2011).

[16] K. A. Taipale, "Cyber-Deterrence," in *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization*, ed. Pauline C. Reich. (Hershey: IGI Global, 2009), 38.

[17] Ibid.

National Policy versus Cyber Deterrence, uses these definitions to quickly determine aspects of cyber deterrence addressed, and also show areas that still require further development. For deterrence to work the adversary must be made aware of the capabilities available for retaliation, the punishment exacted in response is credible, that they will be identified once an attack is made, and that they will be held accountable for their actions.

CHAPTER 2: POLICIES AND DIRECTIVES

Overview

This chapter explores the various policies and directives that establish the current posture of the United States government towards cyber defense and how they contribute to cyber deterrence policy. Although current policy regarding cyberspace is still being crafted and updated, this chapter provides a snapshot of current roles and responsibilities for the defense of cyberspace and the cyberspace connected infrastructure. A general understanding of national security policies toward the defense of cyberspace is important in the comparison of executed cyber-attacks, and how well these documents relate toward a posture of cyber deterrence. In this chapter is an analysis of each document as it relates to Department of Defense and Homeland Security roles and responsibilities toward deterrence in cyberspace and critical infrastructure. The policy documents examined in this chapter define the y-axis of Table 1 - National Policy Shortfalls Tool. The policy documents are categorically divided by the issuing authority and purpose.

Executive Directives, National Strategies, and Departmental Directives

As nations and individuals continue to increase the connections to cyberspace, the need to provide secure and reliable access has also increased. The ensuing policy document summaries focus on those providing guidance and direction relevant to the protection of cyberspace and critical infrastructure. At the executive and national level, these documents leverage all instruments of national power: Diplomatic, Information, Military, and Economic (DIME). Nested within these documents are the strategies, policies, and plans of the Department of Defense and Department of Homeland Security that provide guidance and direction to the organizations charged with the protection of cyberspace and critical infrastructure. At the

highest level is the National Security Strategy (NSS) which articulates the President's strategic direction of the national security effort. In support of the NSS the Secretary of Defense promulgates a National Defense Strategy (NDS) further defining the strategic direction of the DoD which enables the Chairman of the Joint Chiefs of Staff to develop the National Military Strategy (NMS). The NMS utilizes guidance from the NSS, NDS, and current security environment to develop national military objectives for the components. DoD Directives provide guidance to DoD organizations for performing their assigned duties and responsibilities. National plans provide guidance for securing and responding to incidents of national significance. A brief summary of policy documents, plans, and directives related to deterrence in cyberspace along with an analysis of how each either reinforces or fails to address an aspect of deterrence is provided below.

Executive

The National Security Strategy of the United States of America

> Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale.[1]

The National Security Strategy (NSS) of the United States of America 2010 focuses the strategic direction of America in four areas: security, prosperity, values and international order. For security the NSS highlights the need to secure cyberspace through partnerships and investment in research and development.

[1] U.S. President, *National Security Strategy*, (Washington, DC: Government Printing Office, May 2010), 27.

Although a small portion of the NSS is focused towards cyberspace, the document does articulate most of the aspects of deterrence outlined in opening chapter. To increase **dependency** the NSS seeks to strengthen partnerships to include citizens, the private sector, and engagement with the international community.[2] The NSS goes on to articulate how the United States will approach **attribution** and **penalty** to cyber-attacks by "investigat[ing] cyber intrusion … to ensure an organized and unified response to future cyber incidents."[3] The NSS provides some examples of the critical infrastructure vulnerable to attack (e.g. electric grids), but limits the **definition of attack** to "data preservation, protection, and privacy."[4] Highlighted throughout the NSS portion on cyberspace is the idea of resiliency that promotes **futility,** an aspect of deterrence previously discussed. To address **credibility**, the NSS calls for "the development of norms for acceptable conduct in cyberspace; laws concerning cybercrime."[5] By investing in people and technology the NSS is directing efforts at increasing "cybersecurity **awareness.**"[6] Using the National Policy Shortfalls Tool to examine the NSS, there is evidence policy necessary for deterrence in cyberspace is being developed at higher levels of government and may begin to impact future iterations of other documents.

Executive Order 13231 - Critical Infrastructure Protection in the Information Age

Shortly after the September 11, 2001 attacks, Executive Order (EO) 13231- Critical Infrastructure Protection in the Information Age was issued to focus efforts on the protection of information systems and establish a method to recommend and coordinate programs for the protection of critical infrastructure. Also, should measures developed fail to provide adequate

[2] Ibid., 28.
[3] Ibid.
[4] Ibid
[5] Ibid.
[6] Ibid.

protection, any "disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."[7]

The primary focus of EO 13231 is to promote the defense of critical infrastructure susceptible to attack through cyber space. The document primarily seeks deterrence through denial, but does address **awareness** by assigning responsibilities to "work with industry, State and local governments, and nongovernmental organizations to ensure that systems are created and well managed to share threat warning, analysis, and recovery information among government network operation centers, information sharing and analysis centers."[8] EO 13231 tasks its board members with seeking out interdependencies between networks and infrastructure and ensuring their protection, but does not look to increase dependency on the system(s) identified.[9] The document also does not address **attribution, penalty, credibility, definition of attack,** and **futility**. EO 13231 does little to drive toward efforts to defend cyberspace through a policy of deterrence and this is shown by examining the document with the Using National Policy Shortfalls Tool.

National Strategy for Homeland Security

In October of 2007 the White House released the National Strategy for Homeland Security (NSHS) to organize the nation's efforts in the defense of the homeland against terrorist attacks. It identifies strategic objectives and critical mission areas of the Department of

[7] U.S. President, *Executive Order 13231 – Critical Information Protection in Information Age,* (Washington, DC: Government Printing Office, October 16, 2001), 10620.
[8] Ibid., 10623.
[9] Ibid., 10629.

Homeland Security.[10] For each identified critical mission area the NSHS provided initial guidance on how homeland defense would be achieved.

Deterrence through denial is primary way the NSHS seeks to ensure the safety and security of the nation's critical infrastructure.[11] **Penalty** is addressed to change the motivational calculus of would be attackers by holding a host nation, either knowingly or unknowingly, to account. **Credibility** and **attribution** are discussed in our ability to:

> communicate and demonstrate our will to take action, both to our enemies in order to raise their awareness and to the American people so that they remain confident in our resolve. Maintaining our credibility also requires that we not only demonstrate our will … but that we also retain the capabilities and flexibility to do so. This includes enhancing our ability to respond … using all instruments of national power, as well as refining our ability to define the nature, source, and perpetrator of an attack.[12]

Similar to the NSS, **futility** is also included through the resiliency of critical infrastructure and key resources from attack.[13] Using the National Policy Shortfalls Tool to examine the NSHS shows only half the aspects of cyber deterrence policy are addressed and there are additional areas that can be expanded on.

Cyberspace Policy Review

In May of 2009 the White House released the Cyberspace Policy Review (CPR) findings which addressed the potential threats the nation faced with respect to its digital infrastructure. The CPR "outlines the beginning of the way forward towards a reliable, resilient, trustworthy digital infrastructure for the future."[14] It also provides near-term and mid-term action plans to address issues of coordination, direction, and leadership.

---

[10] U.S. President, *National Strategy for Homeland Security*, (Washington, DC: Government Printing Office, October 2007), 13.

[11] Ibid., 26.

[12] Ibid.

[13] Ibid., 28-29.

[14] U.S. President, *Cyberspace Policy Review,* (Washington, DC: Government Printing Office, 2009), iii.

The CPR is another executive document that seeks to better define the **penalty** associated with cyber-attack by "partner[ing] appropriately with Congress to ensure adequate law, policies, and resources are available to support the U.S. cybersecurity-related missions."[15] Aimed at increasing **awareness**, the CPR outlines four avenues of approach: increase public awareness of the risks of online activities, increase cybersecurity education, expand federal information technology workforce, and promote cybersecurity as an enterprise leadership responsibility.[16] To encourage the aspect of **futility** the CPR encourages innovation to focus on ways to increase the resiliency of critical infrastructure and networks "against physical damage, unauthorized manipulation, and electronic assault."[17] Missing from the CPR are the ways to deter cyber-attack through **attribution, credibility, definition of attack, dependency,** and **counter-productivity.** Using the National Policy Shortfalls Tool to examine the CPR needs to better address the aspects of deterrence since only three of eight are addressed.

Comprehensive National Cybersecurity Initiative

The Comprehensive National Cybersecurity Initiative (CNCI) established as part of the January 2008 Homeland Security Presidential Directive 23 and National Security Presidential Directive 54 informs the efforts of the Cyberspace Policy Review. The CNIC articulates 12 initiatives designed to establish a front line of defense against today's immediate threats, establish a front line of defense against today's immediate threats, and strengthen the future cybersecurity environment.[18]

[15] Ibid., 10.
[16] Ibid., 13-15.
[17] Ibid., 31.
[18] U.S. President, *The Comprehensive National Cybersecurity Initiative,* (Washington, DC: Government Printing Office, January 7, 2011), 1.

These initiatives in order presented are: “manage the federal enterprise network as a single network enterprise with trusted internet connections; deploy an intrusion detection system of sensors across the federal enterprise; pursue deployment of intrusion prevention systems across the federal enterprise; coordinate and redirect research and development (R&D) efforts; connect current cyber operations centers to enhance situational awareness; develop and implement a government-wide cyber counterintelligence (CI) plan; increase the security of our classified networks; expand cyber education; define and develop enduring ‘leap-ahead’ technology, strategies, and programs; define and develop enduring deterrence strategies and programs; develop a multi-pronged approach for global supply chain risk management; and, define the federal role for extending cybersecurity into critical infrastructure domains.”[19]

CNIC initiative #2, #5, and #8 place the emphasis on **awareness** and the ability to identify when “unauthorized users attempt to gain access.”[20] Initiative #10 applies the deterrence aspect of **penalty** by “building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.”[21] Using the National Policy Shortfalls Tool to examine the CNCI shows that the document addresses only 25% of the aspects of deterrence defined in Chapter 1.

Homeland Security Presidential Directive 7

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection “establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect

[19] Ibid., 2-5.
[20] Ibid., 2-3.
[21] Ibid., 5.

them from terrorist attacks."[22] HSPD-7 delineates the roles and responsibilities for the Secretary of the Department of Homeland Security and also designates the Department of Defense as the Sector-Specific Agency for the Defense Industrial Base.

Tasked with increasing **awareness** to cyber-attack, the Secretary for Homeland Security will develop a national indications and warning architecture to facilitate "the identification of indicators and precursors to an attack."[23] The document falls short in any further discussion on how to deter an attack other than to continue to increase deterrence through denial. Using the National Policy Shortfalls Tool to examine HSPD-7 shows that most aspects of deterrence applied to cyberspace are largely absent from the document.

National Strategy for the Physical Protection of CI and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (NSPP-CI/KA) provides specific initiatives to identify protection priorities and inform the resource allocation process.[24] Issued in February of 2003 by the White House, it further highlights the importance of a collaborative environment between government, industry, and private citizens in the protection of the nation's critical infrastructure and key assets.

The NSPP-CI/KA goes on to describe a process that will increase **awareness** of an attack throughout federal, state, and local governments and private-sector partners by close collaboration "to develop thorough assessment and alert processes and systems to ensure that threatened assets receive timely advance warnings."[25] Unlike previous national documents the NSPP-CI/KA seeks to implement **futility** through "redundancy within the infrastructure is

[22] U.S. President, *Homeland Security Presidential Directive 7*, (Washington, DC: Government Printing Office, December 17, 2003), 1.

[23] Ibid., 7.

[24] U.S. President, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, DC: Government Printing Office, February 2003), vii.

[25] Ibid., 2.

critical to ensure that single points of failure in one infrastructure will not adversely impact others."[26] Using the National Policy Shortfalls Tool to examine the NSPP-CI/KA shows little to deter cyber-attack against the nation's critical infrastructure, requiring six of eight areas to be addressed.

Department of Defense

The National Military Strategy of the United States of America

> Global Commons and Globally Connected Domains – Assured access to and freedom of maneuver within the global commons – shared areas of sea, air, and space – and globally connected domains such as cyberspace are being increasingly challenged by both state and non-state actors.[27]
>
> We will enhance deterrence in … cyberspace by possessing the capability to fight through a degraded environment and improving our ability to attribute and defeat attacks on our systems or supporting infrastructure.[28]

Issued February 2011, The National Military Strategy (NMS) of the United States of America incorporates the guidance found in the National Security Strategy and the Quadrennial Defense Review (QDR) and develops objectives based on the current security environment. Currently, the national military objectives are stated as:

1. Counter Violent Extremism
2. Deter and Defeat Aggression
3. Strengthen International and Regional Security
4. Shape the Future Force

The NMS calls for collaboration "with U.S. government agencies, nongovernment entities, industry, and international actors to develop new cyber norms, capabilities,

[26] Ibid., 49.
[27] Chariman Joint Chiefs of Staff. *National Military Strategy*, (Washington DC: Government Printing Office, February 8, 2011), 3.
[28] Ibid., 8.

organizations, and skills," and, "executive and Congressional action to provide new authorities to enable effective action in cyberspace."[29]

The Chairman's view expressed in the NMS recognizes cyberspace as a warfighting domain; however, **futility** through resiliency and **awareness** of attack are discussed to leverage the nation's cyberspace offense capability.[30] Using the National Policy Shortfalls Tool to examine the NMS highlights the documents view of cyberspace as a domain to carry out offensive action and only addresses two aspects of cyber deterrence.

Strategy for Homeland Defense and Civil Support

The Strategy for Homeland Defense and Civil Support incorporates guidance found in the National Security Strategy and the National Strategy for Homeland Security. The Strategy for Homeland Defense and Civil Support advocates an "active, layered defense [that] is global, seamlessly integrat[es] US capabilities in the forward regions of the world, the global commons of space and cyberspace, in the geographic approaches to US territory, and within the United States… a defense in depth.[31] The strategy denotes organizational roles, key objectives, and capabilities needed for homeland defense.

The Strategy for Homeland defense and Civil Support limits the discussion of deterrence to increased redundancy of cyberspace connected systems which touches on **futility** as an aspect of deterrence.[32] Also, briefly mentioned is increasing **awareness** through communication between federal, state, and local governments with respect to critical infrastructure protection from attack and recovery. Using the National Policy Shortfalls Tool to examine the Strategy for

[29] Ibid., 10.
[30] Ibid., 19.
[31] U.S. Department of Defense, *Strategy for Homeland Defense and Civil Support*, U.S. Department of Defense, (Washington DC, 2005), 1.
[32] Ibid., 24.

Homeland Defense and Civil Support shows that aspects related to cyber deterrence have room for development within the document.

DoD Policy and Responsibilities for Critical Infrastructure Directive 3020.40

As implementing guidance for the HSPD-7 the Department of Defense issued a directive in 2005 called the Defense Critical Infrastructure Program, which has since been cancelled and replaced with the Policy and Responsibilities for Critical Infrastructure directive in July 2010. The current directive assigns responsibilities for the Defense Critical Infrastructure Program (DCIP), establishes policy and assigns responsibilities for the execution of roles assigned to the Department of Defense, ensures consistency with the National Infrastructure Protection Plan, and designates the Defense Infrastructure Sector Lead Agents (DISLAs) and assigns their specific roles and responsibilities.[33]

The DoD Policy and Responsibilities for Critical Infrastructure Directive 3020.40 continues in the same vain as most of the preceding national level documents that simply focus on the **awareness** aspect of deterrence, but does little to articulate any other aspect described.[34] The focus is on identification and protection responsibilities from physical attacks carried out by terrorist organizations. Using the National Policy Shortfalls Tool to examine the DoD Policy and Responsibilities for Critical Infrastructure Directive shows a lack of addressing the majority of the aspects associated with cyber deterrence.

Defense Industrial Base: Critical Infrastructure and Key Resources SSP

In a coordination effort with the National Infrastructure Protection Plan issued by the Department of Homeland Security and as directed by Homeland Security Presidential Directive 7

[33]William J. Lynn III, *DoD Policy and Responsibilities for Critical Infrastructure*, U.S. Department of Defense, (Washington DC: Department of Defense, July 1, 2010), 1.

[34] Ibid., 13.

(HSPD-7), the Department of Defense (DoD) issued the Defense Industrial Base: Critical Infrastructure and Key Resources Sector Specific Plan. As the designated Sector-Specific Agency (SSA) for the Defense Industrial Base this Sector Specific Plan "represents the DoD's effort to describe a vision and methodology to identify critical assets, assess risk, and improve risk management within the sector."[35]

Research and development efforts directed in the Defense Industrial Base: Critical Infrastructure and Key Resources Sector Specific Plan call for "resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems,"[36] that could potentially frustrate a would be attacker into thinking the result of an attack was of little consequence and therefore prove **futile**. A focus on communication between government agencies and the private sector, **awareness**, is also threaded throughout the plan. Using the National Policy Shortfalls Tool to examine the Defense Industrial Base: Critical Infrastructure and Key Resources Sector Specific Plan highlights a similar lack of addressing the key policy aspects shared with previous documents regarding deterrence in cyberspace.

Department of Defense Strategy for Operating in Cyberspace

Issued in 2011, the Department of Defense Strategy for Operating in Cyberspace provides strategic initiatives in an effort to capitalize on cyberspace as a warfighting domain.

> The Department and the nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity – the security of the technologies that we use each day. Moreover, the continuing growth of networked

[35] U.S. Department of Defense, *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan*, (Washington DC: Department of Defense, May 2007), 3.

[36] Ibid., 35.

systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission.[37]

The initiatives are designed to leverage DoD capabilities to effectively protect and fight in cyberspace.

There are five strategic initiatives in the DoD Strategy for Operating in Cyber space, two directly contribute towards a policy of deterrence. The five initiatives in order presented are: "treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential; employ new defense operating concepts to protect DoD networks and systems; partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy; build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity; and, leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation."[38]

Strategic initiative #3 seeks to raise **awareness** through a "whole-of-government cyber security strategy" that will enable the government and private sector to better identify attacks.[39] Engagement with the international community is the focus of strategic initiative #4 which lends **credibility** to a collective deterrence approach with established **penalties** and norms designed to **define a cyber-attack**.[40] Using the National Policy Shortfalls Tool to examine the Department of Defense Strategy for Operating in Cyberspace shows only half of the aspects of deterrence in cyberspace are considered.

[37] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* (Washington DC: Department of Defense, July 2011), 1.
[38] Ibid., 5.
[39] Ibid., 8.
[40] Ibid., 9.

Department of Homeland Security

National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace, issued by the DHS in February 2003, "is an implementing component of the *National Strategy for Homeland Security* and is complemented by a *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*."[41] The document establishes strategic objectives, priorities for the protection of cyberspace and critical infrastructure, and the initial framework necessary to engage the private sector in the effort to prevent and respond to cyber-attack. The National Strategy to Secure Cyberspace also attempts to delineate the roles and responsibilities at each level of interaction with cyber space from the home user (e.g. a PC connected to the internet) through the global level (e.g. the global economy). It highlights the need to engage the private sector in the safety and security of cyberspace and recognizes the importance of a partnership to that end.

National Strategy to Secure Cyberspace asserts "the United States now requires a different kind of national response system in order to detect potentially damaging activity in cyberspace."[42] This assertion is made through comparison of the federal government's efforts (under nuclear deterrence policy) to protect the nation through the creation of a network of radars designed to provide advanced warning from aircraft and missile attack. The level of **awareness** needs to be of a level sufficient to signal an adversary the attack will be detected in time to take action. The strategy recognizes the role the various law enforcement agencies play in the **attribution** of an attack to apprehending and swiftly bringing to justice the responsible individuals," which "can stem the tide of an ongoing attack and lessen the harm that is ultimately

[41] U.S. Department of Homeland Security. *National Strategy to Secure Cyberspace*, (Washington, DC: Department of Homeland Security, 2003), vii.

[42] Ibid., 19.

caused."[43] **Credibility** through the engagement of the international community is part of the fifth priority outlined in the strategy:

> Systems supporting this country's critical national defense and the intelligence community must be secure, reliable, and resilient—able to withstand attack regardless of the origin of attack. America must also be prepared to respond as appropriate to attacks against its critical infrastructure. At the same time, America must be ready to lead global efforts, working with governments and industry alike, to secure cyberspace that is vital to the operation of the world's economy and markets. Global efforts require raising awareness, promoting stronger security standards, and aggressively investigating and prosecuting cybercrime.[44]

Since there is no geographical border in cyberspace, the strategy articulates the need to have a cooperative approach to deterring attacks in cyberspace. In addressing imposing a **penalty** the National Strategy to Secure Cyberspace "United States reserves the right to respond in an appropriate manner," and "when a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution."[45] Similar to the Department of Defense Strategy for Operating in Cyberspace, the National Policy Shortfalls Tool shows only half of the aspects of deterrence in cyberspace are in the Department of Defense Strategy for Operating in Cyberspace.

National Infrastructure Protection Plan

Based on the requirements in the HSPD-7 the Department of Homeland Security released the National Infrastructure Protection Plan (NIPP) in 2009. The NIPP guides effort in the integration of critical infrastructure and key resources protection between federal, state, local, and private sector entities.[46] Within the NIPP a federal agency known as Sector-Specific

[43] Ibid., 28.
[44] Ibid., 49.
[45] U.S. Department of Homeland Security. *National Strategy to Secure Cyberspace*, (Washington, DC: Department of Homeland Security, 2003), 65.
[46] U.S. Department of Homeland Security. *National Infrastructure Protection Plan*, (Washington, DC: Department of Homeland Security, 2009), 5.

Agency is designated to lead critical infrastructure protection efforts for 18 identified critical infrastructure sectors.

The NIPP has a multifaceted approach to protecting the nation's infrastructure including the coordination of national efforts to raise **awareness** of precursors of an attack in cyberspace.[47] By "developing or encouraging appropriate protective measures, information-sharing mechanisms, and emergency recovery plans for cyber assets, systems, and networks within the sector and interdependent sectors," the NIPP discusses a path toward render attempts against the nation's infrastructure **futile**.[48] Engaging international partners and fostering new diplomatic relationships to ensure attacks that originate in other countries can be investigated and suspects apprehended supports the deterrence aspect of **credibility**.[49] Using the National Policy Shortfalls Tool to examine the NIPP shows 63% shortfall when addressing aspects of deterrence as applied to cyberspace.

Summary

> Developing a comprehensive cyber deterrence will by no means be easy to achieve and will take lots of patient work. Just because our Cold War deterrent strategy is no longer applicable and a replacement is not immediately obvious it does not mean we should conclude that cyber deterrence is impossible. After World War II and the introduction of nuclear weapons, policy makers took time to develop the sustainable framework of mutually assured destruction. This strategy was not immediately obviously at the dawn of the Cold War and we should therefore not expect that a cyber deterrent strategy will also be immediately obviously.[50]

This chapter provided an analysis of the national orders, strategies, directives, and plans that lead towards the establishment of a policy of deterrence by the United States as a strategy to

[47] Ibid., 17.
[48] Ibid., 20.
[49] Ibid., 56.
[50] Ned Moran, "Achieving Cyber Deterrence," The Cuckoo's Egg, http://gucosc011.blogspot.com/2009/04/achieving-cyber-deterrence.html (accessed February 26, 2012).

defend its critical infrastructures from attack originating in cyberspace. While many of the documents advocate certain aspects of deterrence, there is no document subordinate to the National Security Strategy that implements a majority of the aspects previously discussed. The National Policies Shortfall Tool shows that, of the fourteen documents considered in this chapter compared to the eight aspects of deterrence defined in Chapter 1, more than two-thirds of the deterrence aspects go unaddressed. The NSS provides a good foundation, but the documents written to support the defense of the nation's interests in cyberspace are dated and require substantial revision to which to build a policy focused on cyber deterrence.

CHAPTER 3: CYBER-ATTACK

Overview

This chapter will cover examples where cyberspace has been used as an avenue of approach in conducting a cyber-attack and apply the aspects of deterrence (penalty, credibility, definition of attack, dependency, counter-productivity, awareness, and futility) previously discussed. As an alternative to a conventional attack, a tool to coordinate efforts of a lesser force on the battlefield to amplify its effectiveness, or as a pre-emptive strike in a state versus state conflict the use of cyberspace requires special attention. While the possibility to deter these types of attacks can be through denial (defense) the importance of developing a policy of deterrence by punishment (threat of penalty) can greatly enhance the protection of the United States' ability to secure cyberspace. The following examples draw similarities to the types of threats the United States potentially faces in cyberspace and highlights the need for the development of policy toward deterrence in cyberspace.

Stuxnet - Background

In June of 2010 malicious code was discovered by a security firm which was designed to infect industrial equipment.[1] After investigation by the computer security community into how the code worked it was discovered that it specifically targeted Siemens industrial SCADA systems running Microsoft Windows operating systems.[2] Infected systems found to be located in Iran and reports of reduced operational capacity and replacement of nearly 1000 nuclear

[1] Kupreev Oleg, and Ulasen Sergey, *Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review,* Technical Paper, (Minsk: VirusBlokAda, 2010), 7.

[2] TrendMicro. "Stuxnet Malware Targeting SCADA Systems." TrendMicro, http://threatinfo.trendmicro.com/vinfo/web_attacks/Stuxnet%20Malware%20Targeting%20SCADA%20Systems.html (accessed November 13, 2011).

centrifuges used for uranium enrichment at the Natanz nuclear facilities highlight the effectiveness of the virus and its ability to propagate.[3]

This computer worm (malware), named Stuxnet, is initially introduced into a computer system via a portable USB device and then spreads throughout the network looking for very specific control systems.[4] Once the infected USB device is introduced to the network, the virus begins by manipulating a Windows based platform used by a maintenance engineer to configure real-time control systems.[5] Once the Stuxnet virus infects the correct network, the virus manipulates the control drive speeds and valves to damage the centrifuges, see Figure 3-1.

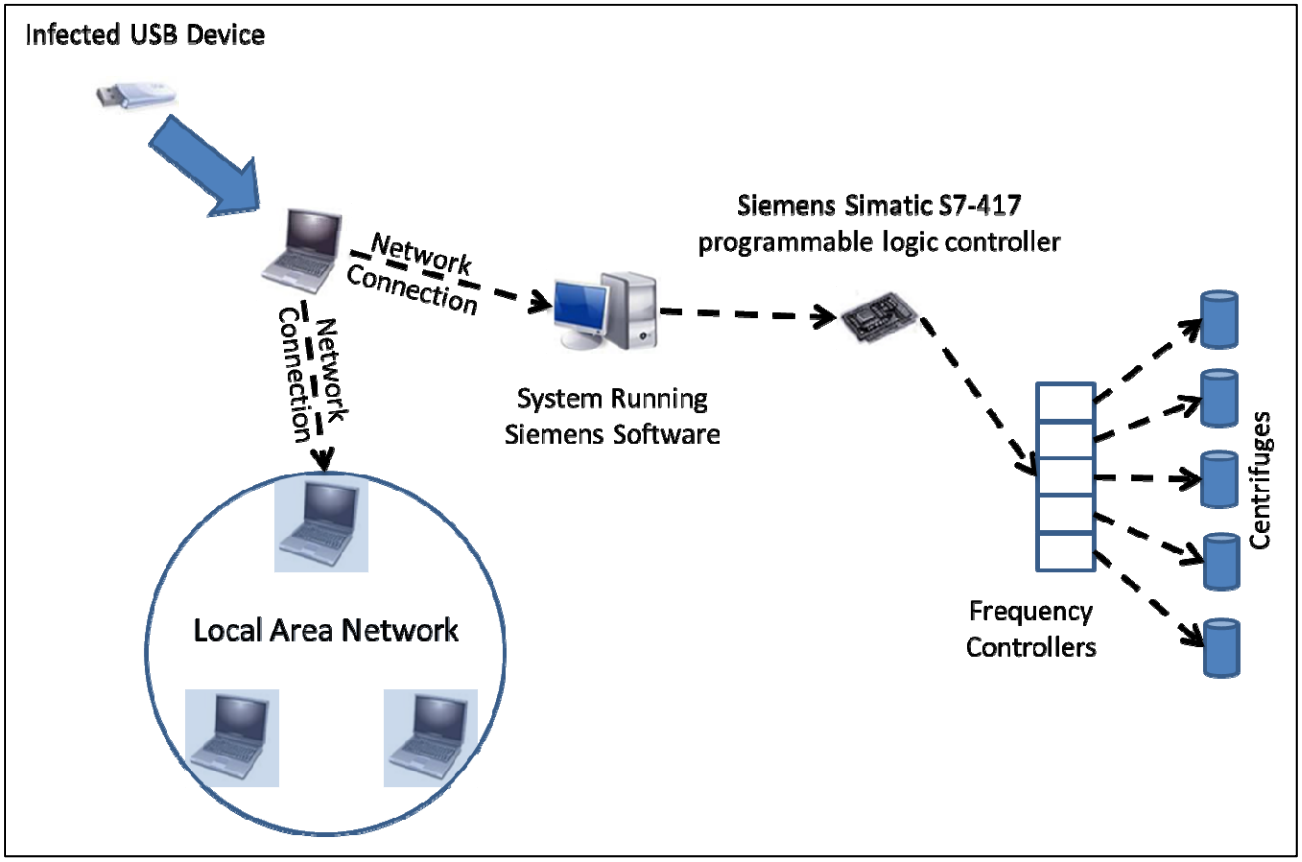


Figure 3-1 - How Stuxnet Propagates

[3] British Broadcasting Corporation, "Iran says nuclear programme was hit by sabotage," British Broadcasting Corporation, http://www.bbc.co.uk/news/world-middle-east-11868596 (accessed November 13, 2011).

[4] Malware - software that is intended to damage or disable computers and computer systems.

[5] Ralph Langner, *Cracking Stuxnet, a 21st-century cyber weapon*, TED, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (accessed May 24, 2012).

While it is unproven the specific target was the uranium enrichment infrastructure in Iran, the end result was a demonstration of a highly successful cyber-attack of unknown origin; however, the complexity in design and the resources used to deploy Stuxnet suggest that it was carried out by a nation state with advanced cyber capabilities and specific knowledge of the Iranian uranium enrichment program.[6]

From Worm to Cyber-Weapon

Unlike most modern malware that is used in criminal activities such as key-logging, spam emails, and denial-of-service attacks, the Stuxnet code was written specifically for the sabotaging of industrial equipment. Once Stuxnet is in place it is designed to adjust the speed of the centrifuge rotors and to manipulate valves that would prevent damage to components.[7] While affecting the performance of the centrifuges, it provides the control systems with false information that is already pre-programmed preventing any type of automated safety response to provided protection. Stuxnet was able to remain undetected by only making small changes in the system that would go unnoticed by operators. As a result of the varying changes in speed of the rotors excessive wear and failure of the centrifuges resulted. Not only was there mechanical damage, but the uranium that was enriched was done so incorrectly and was contaminated to a point it would have to be re-processed.[8]

[6] British Broadcasting Corporation, "Iran says nuclear programme was hit by sabotage," British Broadcasting Corporation, http://www.bbc.co.uk/news/world-middle-east-11868596 (accessed November 13, 2011).

[7] Ralph Langner, *Cracking Stuxnet, a 21st-century cyber weapon*, TED, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (accessed May 24, 2012).

[8] Kim Zetter, "Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage," Wired, http://www.wired.com/threatlevel/2010/11/stuxnet-clues/ (accessed May 21, 2012).

Discovery

Once a significant portion of the centrifuges at the Natanz facility began to fail measures were taken that limited the amount of damage caused by the Stuxnet virus. Large portions of the facility were shut down for extended periods until the virus was discovered publicly. Had the virus gone undiscovered the potential existed for a significant delay and re-evaluation of the Iranian ability to successfully enrich uranium. While the Iranian government admits the cause of failure at the Natanz facilities was due to a computer worm they have publicly downplayed the impact the Stuxnet virus had on their operations.

Aspects of Deterrence Applied

Attribution – it is the opinion of the experts that there are only a few entities capable of carrying out such an attack, and even fewer that have the motivation.[9] The Iranian government is unwilling to admit the virus had an impact and as a result they are unlikely to attribute the attack to a specific adversary.[10]

Penalty – as a result of the unwillingness of the Iranian government in attributing the damage to their nuclear enrichment facilities, the threat of penalty is minimized.[11] Had the Iranian government been willing to admit the destruction of the centrifuges at Natanz to the international community they may have been able to pursue legal action.

Credibility – as previously defined for a policy in deterrence to be effective it must be credible. With the success of the Stuxnet virus and no documented or visible response from the Iranian government the credibility they have to deter future cyber-attack is lost. Assertions by

[9] Ralph Langner, *Cracking Stuxnet, a 21st-century cyber weapon*, TED, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (accessed May 24, 2012).

[10] Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," NDU Press, http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html (accessed May 21, 2012).

[11] Ibid.

Iranian officials that "the country's young experts stopped the virus exactly at those points that enemies intended to infiltrate," diminish the credibility of significant response even further.[12]

Attack definition – "Stuxnet is like a self-directed stealth drone: the first known virus that, released into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done."[13] Due to the nature in which the virus manipulated the data systems to disrupt enrichment and subvert the information passed to operators, Stuxnet was in the data disruption category.

Awareness – the way in which the Stuxnet virus operated limited the opportunities for discovery. Had the international community not discovered the virus, it is likely that replaced centrifuges would have failed in similar fashion.

Futility – based on the communications from Iranian officials the attempt to indicate the futility of the attack does not correspond with the physical actions taken to recover from the incident.[14]

Stuxnet Summary

If the speculation proves to be correct and the originator of Stuxnet was a cyber-super power, it should raise concerns about the ability of the Iranians to continue secret operations towards developing nuclear material. It suggests that external intelligence agencies demonstrated their ability to infiltrate programs of national importance to the Iranian government and dismantle them while providing no means of detection.

[12] FARS "Commander Stresses Iran's Capability to Repel Cyber Attacks," FARS News Agency, http://english.farsnews.com/newstext.php?nn=9004170896 (accessed May 23, 2012).

[13] Michael J. Gross, "A Declaration of Cyber-War," Vanity Fair, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104 (accessed May 22, 2012).

[14] FARS "Commander Stresses Iran's Capability to Repel Cyber Attacks," FARS News Agency, http://english.farsnews.com/newstext.php?nn=9004170896 (accessed May 23, 2012).

Unlike a conventional attack against Iranian nuclear facilities a cyber-attack causes the same result while limiting the threat of retribution, and demonstrates the use of software as a decisive weapon. While Stuxnet is seen to be a cyber-attack specifically directed toward Iran, the "Pandora's box" of cyber warfare may have been opened.

Cyberspace: An Insurgency Force Multiplier

Two types of actions are key components of insurgency doctrine: covert action in urban areas, and organized media action.[15] Prolonged conflict in Iraq and Afghanistan have highlighted the insurgent's effectiveness in employing improvised explosive devices as the primary means to conduct armed conflict against coalition forces. To develop mass mobilization the insurgents have capitalized on internet capabilities to recruit, inform, plan, and develop targets. This has redefined the battlefield for the commander by increasing the insurgent's ability to rapidly communicate a narrative that may be contrary to actual events to adversely influence public opinion.

While there are no physical attacks carried out in cyberspace, the ability to communicate via the web, cell phones, and other electronic means has allowed the insurgents to more effectively win the "hearts and minds" of the population to maintain the support of sympathizers.[16] The use of cyber activities by the insurgents in Iraq and Afghanistan could be likened to the "Min Yuen" of the Malayan Emergency between the British Empire and insurgents

[15] Michael Scheuer, "Al-Qaeda's Insurgency Doctrine: Aiming for a 'Long War'," The Jamestown Foundation, http://www.jamestown.org/programs/gta/single/?tx_ttnews%5Btt_news%5D=690&tx_ttnews%5BbackPid%5D=239&no_cache=1 (accessed May 22, 2012)

[16] Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping*, (New York: Stackpole, 1971).

in Malaysia, or at least it provides a readily available conduit to communication between the two.[17]

Civilian Mass Mobilization

Leading up to the wars in Iraq and Afghanistan the ability to rapidly mass force through organized media action was demonstrated during protests of the World Trade Organization in 1999. During the protesting, a call for public support went out over the web from human rights groups, students, environmental groups, religious leaders, and labor rights activists generating a massive showing which effectively thwarted police efforts to contain public demonstrations, by utilizing the live media coverage to quickly reposition to areas that were largely unprotected.[18] This same tactic used to better organize protesters allows terrorist organizations to use relatively inexpensive communications equipment to monitor the battle space and allow for rapid movement and maneuver of largely inexperienced forces providing a significant advantage in staying ahead of the fight. Today, rapid communication and the ability to mobilize the population is demonstrated by the Arab Spring and the overthrowing of the Muammar Gaddafi regime. Extremists and sympathizers are able to communicate over various cyber mediums generating additional resources instrumental in maintaining an insurgency.

Exchange of Communication

Relying on social media, the portability and reliability of mobile devices, and the increasing degree to which anti-coalition forces have access have been instrumental to the maintenance of insurgencies. The effect of the communications and education on the population

[17] Paul Melshen, "Mapping Out a Counterinsurgency Campaign Plan: Critical Considerations in Counterinsurgency Campaigning," *Small War and Insurgencies* 18, no. 4 (December 2007), 665-698.

[18] Paul de Armond, "Netwar in the Emerald City: WTO Protest Strategy and Tactics," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 201-235, ed. John Arquilla, & David Ronfeldt, (Santa Monica: RAND, 2001), 54.

through the cyber medium has been instrumental in maintaining a voice outside the conflict to garner new recruits. Due to the anonymous nature of the internet, both men and women can participate equally in their support of an insurgency. This tool turned weapon helps to define a narrative counter to reality that continues to draw support and enables mass mobilization.

The low cost of entry into cyber-space allowed the insurgents in Iraq and Afghanistan to successfully combat coalition information operations forces who had a significant advantage in resources, doctrine, and training. There are various reasons the insurgents were able to gain the upper hand. Chiefly among them was they were the aggressor and often had the narrative pre-written and available for dissemination prior to any actual attack. The absence of a chain of command to acquire release authority prior to transmission also enabled the quick change of narrative should an attack fail.[19] For the population the first report is usually the report acted upon, and as a result coalition forces, with complex chains of command, are usually held responsible in the court of public opinion.

The expansion in numbers of insurgent websites and increased regional reporting has allowed the Iraq and Afghanistan insurgents to espouse the extremist points of view and manipulate the population in an effort to undermine the partnership between legitimate police forces in both Iraq and Afghanistan and collation forces. Keeping the population safe is an important aspect in defeating an insurgency, but the insurgent's ability to develop a picture that places the blame on coalition forces results in continued support for the insurgency and a desire for coalition forces to withdraw.[20] This type of disinformation has always been part of an

[19] Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," Military Review (May-June 2006), 13-32.

[20] David Nakamura, "Afghans blame civilian deaths on U.S. despite spike from insurgent violence," The Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/13/AR2010081305821.html (accessed May 19, 2012)

insurgency strategy, but the utilization of cyber capabilities has multiplied the insurgents' information operations campaign effectiveness.

Redefining the Battlefield

The enemy's use of cyberspace shortens the time the commander's has to observe, orient, decide, and act. The commander's "coup d'oeil"[21] as classically articulated by Clausewitz is fundamentally changed when trying to maneuver through the modern cyberspace influenced battlefield. The fog of war is exacerbated by the insurgent's ability to remain invisible until executing an attack. The commander has the ability to observe and orient, but he must decide and act in the cyber realm, sometimes within milliseconds. Insurgents are able to initiate an attack then rapidly communicate a narrative to a wide audience that views the reports as credible before the commander can react to the event. This new domain of information war fighting allows an insurgent the opportunity to gain an advantage even from an operation that failed to meet its objectives.

The initial focus for defense against cyber related attacks against coalition forces were protecting networks and allowing freedom of movement in cyberspace.[22] The insurgents never employed this type of tactic and most likely recognized early on that any attempt to infiltrate coalition networks would prove to be ineffective and in some cases counter-productive. Allocating resources to attack a well-defended capability would waste time and show little usefulness in spreading their message to elicit support. Not having the restriction to report the truth allows freedom of movement in cyberspace by the insurgents that legitimate coalition forces do not have. Due to the relatively simple message the insurgents are trying to disseminate it is easy for any member, at any level, to quickly generate a report that supports the cause. The

[21] Carl Von Clausewitz, *On War*, (New York: Alfred A. Knopf, 1993), 578.
[22] Bruce Hoffman, *The Use of the Internet by Islamic Extremists,* (Santa Monica: RAND, 2006), 7.

employment of cyberspace to promote the insurgency in this way has allowed its supporters to provide a steady stream of disinformation at very little cost with fewer individuals than the massive effort seen by coalition forces.[23] Not only are insurgents able to quickly disseminate information regarding successful attacks, but they are also able to more effectively communicate potential targets through the cyber medium. A photo can be instantly shared, videos of defenses can be streamed near real time, and this information is difficult to prevent from being obtained.

Aspects of Deterrence Applied

Penalty – the penalty associated with the use of the internet as a means to communicate with the intent to incite lawlessness could be similar to those penalties used to punish an offender that falsely shouting fire in a theater.[24] Not only should the protection of freedom of speech afforded by the First Amendment extend to communications in cyberspace, but also should the First Amendment limitations.

Credibility – due to the fact that cyberspace can be accessed from nearly any point on the globe, the international community will have to adopt policy that lends credibility to any associated penalty.

Summary of Cyberspace: An Insurgency Force Multiplier

Using the past to frame the future would suggest that the lessons learned during the wars in Iraq and Afghanistan should not be lost. While the United States is capable of meeting any adversary on the field of battle conventionally and winning, the likelihood of an adversary using conventional means is small for the foreseeable future. The ability for a conventionally superior opponent to bring the insurgents to culmination can be difficult. With the ability to rapidly and

[23] Ibid., 11.
[24] Schenck v. United States, 249 U.S. 47 (1919).

effectively communicate, generate support, sympathy, and recruit not the sole providence of the technologically superior force the insurgents can extend the conflict and potentially wear out their adversary.[25] The use of cyberspace as a force multiplier needs to be taken into account when fighting future wars, both conventional and non-conventional.

Estonia and Georgia - Background

In April of 2007 as a response to the rising tensions between Estonia and Russia, caused by the removal of a Soviet war memorial from Tallinn city center, the first cyber-attack against a nation state began.[26] Estonia is a small Baltic state that is one of the most internet connected countries in Europe. To many Estonians, the statue represented the Soviet occupation and oppression between World War II and their eventual independence in 1981.[27] There was no open conflict between the two governments, just diplomatic tensions which eventually escalated into a series of distributed denial of service attacks from IP address held within Russian borders. As a result of the attacks, Estonia attempted to limit access to its Internet sites from those addresses residing only within the borders of Estonia.[28]

In August of 2008 armed conflict between the Russian Federation and Georgia over South Ossetia, an independent Georgian region along the border of Georgia and Russia. During the Georgian-Ossetian conflict of 1991 South Ossetia declared independence from Georgia, but never gained recognition as an independent state from the international community.

---

[25] Bruce Hoffman, The Use of the Internet by Islamic Extremists, (Santa Monica: RAND, 2006), 24.

[26] Patrick Jackson, "The cyber raiders hitting Estonia." British Broadcasting Corporation, http://news.bbc.co.uk/2/hi/europe/6665195.stm (accessed February 25, 2012).

[27] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (accessed February 25, 2012).

[28] The Economist, "Estonia and Russia: A Cyber-Riot," The Economist, http://www.economist.com/node/9163598 (accessed February 8, 2012).

Unable to resolve the conflict between the two, a peacekeeping force consisting of Russian, Georgian, and South Ossetia's military was formed under the command of the Russian military. However, this peace keeping force was unable to cooperate and, eventually, tensions between Russian supported separatists and Georgia caused the Georgian army to attack separatist forces in 2008.[29]

The Georgian attacks against Russian supported separatists commenced August 7, 2008; and before the day was through cyber-attacks were already in progress against many Georgian government websites. Unlike the political dissent which pre-empted the cyber-attacks mentioned earlier against Estonia in 2007, attacks in cyberspace preceded and combined with political and military action against Georgia.[30]

Estonia's and Georgia's Cyberspace Dependency

As previously mentioned, Estonia is one of the most wired countries in Europe where almost all banking and government activities are conducted on-line, and more than 80% of the population files taxes via the internet.[31] In March of 2007 Estonia held their political elections on-line as well. In comparison to other countries, Georgia, in 2008, had minimal dependence on cyberspace. It is estimated that for every 100 people in Georgia there are approximately seven Internet users.[32] This is in stark contrast to the roughly 57 out of 100 users in Estonia that suffered a similar cyber-offensive a year prior. At the time, Georgia's cyberspace infrastructure, based on geography, was heavily dependent on connections that ran through Russia. There was some capacity to route internet traffic through Turkey, but that in turn was then routed through

[29] Ibid.
[30] Ibid.
[31] Statistics Estonia, "EU Statistics," http://www.stat.ee/international-statistics. (February 2012).
[32] Internet World Stats, "Georgia Internet Usage and Telecommunications Reports," http://www.internetworldstats.com/asia/ge.htm (accessed May 21, 2012).

Russia negating any potential benefit. Estonia, however, did not suffer from the same geographical limitations as Georgia due to the high capacity data links with several other countries as well as agreements with larger network operators to divert excessive traffic to an additional Internet Service Provider.[33]

Cyber-attacks against Estonia and Georgia

The cyber-attacks carried out against Estonia did not attempt to take control of any system or network, but rather prevent the use of political and economic websites. The cyber-attacks against Georgia were primarily of Distributed Denial of Service (DDoS) type, or the manipulation of public websites to communicate false messages or erroneous depictions of political leaders.[34]

On the Georgian Ministry of Foreign Affairs website a collage of various pictures of Adolf Hitler and Georgian President Mikheil Saakashvili were inserted. While the attacks began in earnest after armed conflict began, there is evidence that DDoS attacks had begun as early as July that year.[35] The control server responsible for the DDoS attack on the Georgian president's website were based in the United States and had been in operation for several weeks leading up to the Georgian incursion into South Ossetia.[36]

With the relatively small percentage of the population dependent on the Internet, and the minimal reliance on cyberspace for the operation of Georgia's critical infrastructures, the country experienced little effect beyond the inability to access websites and communicate with

[33] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (accessed February 25, 2012).

[34] John Markoff, "Before the gunfire, cyberattacks," New York Times, http://www.nytimes.com/2008/08/13/technology/13iht-13cyber.15227999.html (accessed January 3, 2012).

[35] Ibid .

[36] Ibid.

sympathizers during the period of armed conflict with Russia.[37] While there are indications of Russian involvement, there is no admission, or clear linkage to Moscow that ties the government of Russia to the attacks.

Aspects of Deterrence Applied

Credibility and Definition of attack – the attacks carried out constitute data disruption and cyber isolation. Addressing data disruption and cyber isolation types of attacks as cyber-weapons has started to gain traction in the international community and will lend credibility to a policy of deterrence.[38]

Dependency – to increase dependency on the Estonia networks, Estonia could encourage the use of Russian participation in the use of their networks. This could have mitigated the desire to disrupt and disable large portions of the government during the conflict.

Counter-productivity – the potential for an advanced, cyber-dependent power overtly to cyber-attack a less dependent adversary if such an attack would legitimize a cyber-response to which the attacker was more at risk because of its own increased dependency.[39]

Futility – the attacks against Georgia were nearly futile due to their relatively small dependence on the internet as previously mentioned, but the attacks against Estonia were significant. Had there been a strategic reserve bandwidth to circumvent these attacks the attacker would have thought his efforts useless.

[37] Ibid.

[38] Paul Marks, "Pentagon readies its cyberwar defences," NewScientist, http://www.newscientist.com/article/mg20126994.600-pentagon-readies-its-cyberwar-defences.html, (accessed March 11, 2012).

[39] K. A. Taipale, "Cyber-Deterrence," in *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization*, ed. Pauline C. Reich. (Hershey: IGI Global, 2009), 38.

Summary of Estonia and Georgia

The cyber-attacks carried out against Estonia highlighted the need for better defenses and additional redundancy in available bandwidth for a country so dependent on the internet. While Estonia could not positively attribute the attacks to Russia, specifically the government, it is doubtful any counterstrike could have been accomplished if positive identification could have been made. With Georgia, at best, the cyber-attacks appear to have been initiated by gangs sympathetic to Russian views on the conflict. The cyber-attacks also represent the first set of attacks that coincided with physical warfare. With Russia overtly sending in ground troops it is more likely that "they could have attacked more strategic targets or eliminated the infrastructure kinetically."[40]

While the cyber-attacks leveled against Estonia and Georgia proved to be of limited value in terms of real world implications, a similar effort that includes physical targets (i.e. critical infrastructure) against a nation dependent on cyberspace could have a significant impact on how a war is fought. The ability to reach out through cyberspace could negate the strategic advantage the United States has in the two oceans. The reach that can be obtained in cyberspace puts United States' critical infrastructure at risk to attack from cyber-attack. The nation's water supplies, rail and traffic control systems, and power grid all use SCADA systems that are proven exploitable.

Why Seek Deterrence in Cyberspace

> Without establishing the identity of the attacker in near-real time, our paradigm of deterrence breaks down. Missiles come with a return address. Cyber-attacks, for the most part, do not. For these reasons established models of deterrence do not

[40] John Markoff, "Before the gunfire, cyberattacks," New York Times, http://www.nytimes.com/2008/08/13/technology/13iht-13cyber.15227999.html (accessed January 3, 2012).

> wholly apply to cyber. We need a deterrent structure that fuses offensive, defensive, and intelligence operations to meet current and future threats.[41]

The low cost of cyber-attack compared to the high cost of cyber-defense makes cyber deterrence an option for policy makers to consider. However, the ways in which deterrence succeeded in the past have not resulted in the same success in cyberspace. Over a six month period the Department of Defense spent over "$100 million dollars reacting to things on [the] networks after the fact."[42] To fully develop a strategy in cyber deterrence policy makers must better define what retaliatory responses are available and against what level of attack will they be employed and continuously evaluate their effectiveness and update as necessary. The type of response to a particular type of attack, either a conventional counterattack, or a counterattack through cyberspace, has to be determined. With a conventional response the possibility of exacting punishment on an innocent third party is likely to create new enemies, and potentially remove the ability to prove the target as the originator of the attack. Alternatively a cyber-counterattack may go unnoticed and provide little in the way of deterring future attacks from other adversaries.

Defining what constitutes a cyber-attack is important to set a baseline for where a strategy of deterrence will be employed. A strategy that has one response, is not scalable, and is predicated on a zero-tolerance policy implies an ability to investigate each incursion, no matter how minor, in the end would prove to be unaffordable. Alternatively, defining a threshold at which an attack would warrant a response could afford an attacker the time necessary to make probative infiltrations into networks to better develop a more devastating attack or disappear altogether.

---

[41] William J. Lynn III, "Stratcom Cyber Symposium," (speech, Omaha, NE, May 26, 2010).

[42] John Davis, "Joint Task Force Global Network Operations Cyber-security Conference," (speech, Omaha, NE. April 2009).

Richard Clarke writes, "A declaratory posture is a formally articulated statement of the policy and intention of the government. We do not have an authoritatively articulated policy today about how we regard a cyber-attack and what we would do in response."[43] This lack of formal declaration of policy relegates the United States response to cyber-attack to one of reaction. Without the fear of reprisal the ability for the United States to shift from defensive to offensive operations in cyberspace becomes limited. While the policy need not be specific, it needs to clearly articulate what constitutes a cyber-attack and what potential resources will be brought to bear.

Developing the freedom of movement through cyberspace is important to furthering the effectiveness of a deterrence strategy. To dominate the environment the ability to seek retribution and infiltrate the adversary's networks and infrastructures is critical to lending credibility to any threats articulated in policy. Relying solely on conventional actions to respond to cyber-attacks maintains the defensive in cyber-space and could prove to be counter-productive to deterring future attacks.

Critical United States Infrastructures Susceptible to Cyber-attack

Over the past few decades the awareness that the nation's critical infrastructure has become increasingly dependent on networks has increased the need to identify and protect these systems.

> As a result of advances in information technology and the necessity of improved efficiency [the nation's critical infrastructures] have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error … and physical and cyber-attacks.[44]

[43] Richard A. Clarke, *Cyberwar*, (New York: HarperCollins, 2010), 187.

[44] U.S. President, *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, (Washington, DC: Government Printing Office, 1998), 2.

While the vulnerabilities of the nation's infrastructure have received increased exposure and as a result has translated into increased protection there will always be available a way to penetrate the defenses.

Water Supplies

The potential to contaminate the nation's water supplies has long been a concern for law enforcement. Although, it is unlikely this form of attack will be carried out by a terrorist organization due to the difficulty in acquiring sufficient quantities of potentially deadly contaminants. However, the ability to inject a computer virus into the control systems of the nation's water utility centers could be easily accomplished. Water utility supervisory control and data acquisition (SCADA) systems are generally not connected to the Internet, and therefore are not prone to a cyber-attack from afar, but could have a virus installed by a disgruntled employee with ties to a terrorist organization.[45]

Power Grid

The nation's power grid is also operated via a networked SCADA system which is susceptible to attack from a potentially modified form of the Stuxnet virus. Not only is the threat of shutting down a concern, but causing actual damage to critical generators and large electric systems is a possibility, potentially causing long term power outages.[46] These attacks have presumably already been introduced to disrupt and damage an Iranian uranium enrichment facility at Natanz. The same type of malicious code has the potential to disrupt portions of the nation's power grid.

[45] Gay Porter DeNileon, "Critical Infrastructure Protection: The Who, What, Why, and How of Counterterrorism Issues," http://www.mrws.org/Terror/Counterterrorism.htm (accessed October 15, 2011).

[46] Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," Cable News Network, http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US (accessed October 15, 2011).

As the power grid continues to age and the reliance on automation to maximize its efficiency, the avenues for approach for cyber-attack grows. SCADA systems have been designed for high efficiency and not high security.[47] As these control systems begin to interact with the Internet they are exposed to the same threats as other computers. Even without the global connection an attack can be carried out through the use of a thumb-drive similar to the attack on the Natanz facility previously mentioned. Even well defended SCADA systems will have vulnerabilities to cyber-attack. Additionally, with the modernization of the electric grid to a "'smart grid' – aimed at improving reliability and efficiency and facilitating the use of alternative energy sources" there is an increased risk that "smart grid systems will be vulnerable to attacks that could result in widespread loss of electrical services." [48]

Rail and Air Traffic Control

The high cost of maintaining a ground based radar system capable of tracking air traffic led to the development of an "Automatic Dependent Surveillance Broadcast (ADS-B) system to increase the capacity and safety of the air transportation system."[49] This system relies on global positioning system (GPS) signals transmitted from aircraft to provide an accurate representation of a plane's identity, ground position, altitude, and velocity to networks of ground stations and other nearby aircraft.

In an effort to design a system simple to operate and cheap to implement the decision was made to leave the transmitted signals unencrypted.[50] This exposes the potential for a hacker to

[47] Andrew Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644 (accessed March 3, 2012)

[48] Gregory C. Wilshusen, "CYBERSECURITY: Challenges in Securing the Modernized Electricity Grid," U.S. Government Accountability Office, (February 28, 2012), 2.

[49] Donald McCallie, Jonathan Butts, and Robert Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection* (2011), 82.

[50] Ibid., 83.

intercept or spoof the aircraft's transmissions. There exists the potential to jam the signal so that a ground receiver could blind air traffic controllers and cause mid-air collisions.[51] Spoofing the transmission may force a pilot to maneuver for an aircraft that in reality does not exist leading to the possibility of collision with something previously not of concern.[52]

The computerized control systems used on the nation's rail systems help coordinate the movement of trains to facilitate transportation of people, ship cargo, and deliver goods. The SCADA networks employed could be infiltrated to cause rail switches to behave erratically or simply cause a failure resulting in a devastating accident if carrying people or hazardous cargo at the time.[53]

Summary

This chapter highlighted examples of the types of cyber-attacks which have already occurred and how the United States is just as susceptible to attack, if not more so based on the dependence on cyberspace with respect to the nation's critical infrastructure. Stuxnet demonstrates the capability to exploit the vulnerabilities of SCADA systems used throughout the nation's critical infrastructure. If an adversary combined the efforts directed against Georgia and Estonia with the capabilities of the Stuxnet virus in disruption of the nation's critical infrastructure the impact on the way of life of the average citizen could be significant. While capabilities of carrying out these types of cyber-attacks against the United States may currently be limited to major cyber-powers, it is unlikely to remain this way in the future. Adversaries must be made aware of the consequences of conducting a cyber-attack against the United States

[51] Ibid.
[52] Ibid.
[53] William T Shaw, "SCADA System Vulnerabilities to Field-Based Cyber Attacks," http://industry consulting.org/pdfFiles/Vulnerabilities%20to%20Field_Based%20Attacks.pdf, (accessed Mar 22, 2012).

and know that they will be identified and held accountable through the articulation of a policy deterrence as applied to cyberspace.

CHAPTER 4: RECOMMENDATIONS

To enforce any policy statement directed at deterrence of cyber-attacks, the United States must continue to develop the ability to detect cyber-attacks, maintain continued access to cyberspace, and preserve the ability to counterstrike. This capability must be demonstrated to work without revealing too much of the "how" so as to not offer the adversary an opportunity to circumvent a U.S. operation. In the cyberspace domain, as shown with the Stuxnet virus, detection and attribution of an attack can be very difficult to determine in a timely manner. The National Policy Shortfalls Tool shows that there are opportunities to improve in the area of cyber deterrence policy and many of the aspects needed to be addressed for a policy of deterrence in cyberspace still require development. While each document does not necessarily need to address each aspect of deterrence, they must be written to support the National Security Strategy toward a policy of cyber deterrence. Most documents are dated and are a reflection of the focus of the nation at the time toward physical attack and not the deterrence of nefarious cyber related activities. However, the nation must continually revise and evaluate current policy to maintain pace with the growing threat presented to the nation's critical infrastructure from attack through cyberspace.

Cyber-attacks that have the potential to be catastrophic in nature so as to threaten the national or economic security of the United States should be the focus of a cyber-attack deterrence policy. Using the definition provided in Joint Publication 1-02, "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the

cost of action outweighs the perceived benefits," [1] a policy of cyber deterrence does not need to address all potential cyber-attacks, but address those that pose a significant threat and alter the adversary's calculus so that they know the attack will be detected, they will be identified, and retaliation will be both swift and credible. An additional consideration in establishing the credibility of deterrence is that the command and control associated with a counter attack is redundant and not dependent on the networks' continued operation.

Articulating that a retaliatory response to cyber-attack need not be limited to cyberspace will be an important aspect of the policy statement. Although the Geneva Convention Law of Armed Conflict does not explicitly define armed conflicts as to include cyber-attacks, the outcome from a successfully executed cyber-attack may have the same affect and therefore subject to the same penalties. Cyber-attacks can make estimating physical level of suffering difficult and need not be solely associated with the established meanings of death, injury, damage, and destruction. The effect on the population should be considered in the retaliation to a cyber-attack and not limited to cyberspace. Currently, there are nations whose reliance on cyberspace is limited. The policy statement aimed at deterring a cyber-attack should include language that does not restrict retaliation to cyberspace alone. Retaliation to a cyber-attack carried out against the nation's power grid, water supply, or other critical infrastructure could be the physical targeting and destruction of similar capabilities of the adversary. For example, an enemy cyber-attack that destroys a water treatment facility can be targeted and destroyed by a conventional attack if the level of attribution is sufficient. This will expand the threat of retaliation to nations that seek to exploit a vulnerability that is asymmetric in nature.

[1] William E. Gortney, "Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms," (Washington, DC: Department of Defense, 2012), 96.

To further a policy in cyber deterrence the United States must begin to publicly demonstrate its cyber offensive capability. Potential adversaries must be made aware that the United States can inflict significant damage in cyberspace and is willing to respond kinetically to any perceived cyber threat or attack. This can be done without alerting the enemy to specifics on how it will be accomplished similar to how the United States' Nuclear Triad is known to be the deterrent to nuclear warfare. Currently, the United States' cyber capabilities are largely secretive. While a potential adversary understands kinetic capabilities of the United States and are deterred from aggression, their ignorance of United States cyber capability invites cyber-attack.

While attribution is a difficult aspect to prove as applied to who to counterstrike, it need not be the reason deterrence fails. Identifying where the attack came from is crucial to lending credibility to a counterstrike, but not to the level necessary in a court of law. Depending on the level of criticism the United States is willing to accept, both domestically and internationally, there is reasonable expectation based on the United States' intelligence collection capabilities that a cyber-attacker can be identified. If the cyber-attack represents a significant impact to the nation's critical infrastructure or as a prelude to a larger conflict the threshold for identification may not need to be to proven beyond a reasonable doubt, but proven to be most likely. This approach could enable the United States' to shift the burden of proof to the adversary where attribution is most likely. There does however exist the real possibility that a cyber-attack seeming to originate within the borders of one country in fact originated in another.

Exploring the legal aspects of cyberspace deterrence policy is an area that deserves further study, and was not included in this paper. Additional areas not fully developed in this paper, but worthy of further study are defining what agency or organization should be vested

with the primary responsibility and authority for cyberspace offensive and defensive operations? Because there are no borders are the geographic limitations imposed on the Department of Justice and Central Intelligence agency appropriate for cyberspace?

The National Security Strategy of the United States is a good beginning to a policy of deterrence in cyberspace. However, the documents that lend granularity to the President's position with respect to cyber deterrence are dated and are focused on deterrence through denial versus deterrence through penalty.

> History teaches us that a purely defensive posture poses significant risks… When we apply the principle of warfare to the cyber domain, as we do to sea, air, and land, we realize the defense of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary, to deter actions detrimental to our interests.[2]

Deterrence in cyberspace needs continuous attention, not only through a credible defensive capability, but also credible offensive capability that can take the fight to the enemy.

Going forward, the United States must continue to develop its ability to defend against cyber-attack, but not become reliant solely on a defensive posture. There will always be an avenue of approach into cyberspace for an adversary to exploit. Convincing a dedicated adversary that to do so would be too costly is, therefore, the best way to ensure the protection of the nation's critical infrastructure.

[2] James Cartwright, "Cyberspace: House Armed Services Committee," (speech, Washington, DC, March 21, 2008).

CONCLUSION

Historical efforts to deter an adversary from attack have been largely effective because of the physical nature of the attack, the well-developed forensics employed to identify the originator of the attack, and the punishment imposed once apprehended or retaliation once identified. In cyberspace, attacks are difficult to trace to the originator, and as a result of this fact coupled with the low cost associated with an attack in cyberspace, the volume of daily cyber-intrusions and cyber-attacks are more than any single law enforcement body can effectively combat. Establishing a policy that raises the likelihood of identification, which in turn increases the relative cost of entering cyberspace for criminal activity, will begin to deter attacks and lead to a more manageable problem set for law enforcement. Once cyber-attacks begin to target the nation's critical infrastructure the ability to quickly identify the origins, determine their impact, and punish the offender(s) will be important to deterring further attempts.

Chapter 1 examined the aspects involved with the theory of deterrence and how they each individually contribute. For deterrence to work the adversary must be made aware of the capabilities available for retaliation, the punishment exacted in response must be credible, that they will be identified once an attack is made, and that they will be held accountable for their actions. Also discussed are a few of the mechanisms available to implement deterrence in cyber space: penalty which focuses on retaliation, futility which makes the adversary view the attack as having very little effect, and dependency which relies on the inter-connectedness of today's global infrastructures.

Chapter 2 provided a summarization of the national orders, strategies, directives, and plans that lead towards the establishment of a policy of deterrence by the United States as a strategy to defend its critical infrastructures in cyberspace. There are numerous documents that

explain each agency's responsibility in defending cyberspace and the nation's critical infrastructures and key assets. Chapter 2 compared the national documents against the aspects of deterrence discussed in Chapter 1 to analyze if there was any additional guidance required for an effective policy of deterrence in cyber space to exist.

Highlighted in Chapter 3 were examples of the types of cyber-attacks that have already occurred and how the United States remains just as susceptible, if not more so, because of the dependence on cyberspace with respect to the nation's critical infrastructure. While adversaries capable of carrying out these types of cyber-attacks against the United States are currently limited, it is unlikely to remain this way in the future. Adversaries must be made aware of the consequences of conducting a cyber-attack against the United States and know that they will be identified and held accountable.

For cyber deterrence to be effective, a policy that clearly articulates the types of cyber-attacks that will face retaliation, and credibly defines the threshold a cyber-attack must meet in terms of disruption or damage, must be issued. This policy statement should be targeted towards nation state actors and non-nation-state actors alike due to the relative ease of access to cyberspace. Fortunately, at this time there is little evidence to support the idea of a non-nation state actor with the means to conduct large scale attacks against the United States. But, similar to the threat of WMDs being acquired and employed by non-nation state actors that have no fear of retaliation, the threat may one day become real.

The application of nuclear deterrence policy developed during the cold war may not be the answer needed to solve a similar problem faced in cyberspace. The access and cost associated with entry into cyberspace are different than those associated with entry into nuclear weaponry. However, the aspects of deterrence are universal in their application, and policies that

support the National Security Strategy must better define how the United States fights, not only in the physical realm of land, air, sea, and space but also in cyberspace. Critical to defending the nation's use of cyberspace will be the ability to influence decisively the mental calculus of potential adversaries to dissuade them from conduct that threatens the United States and its interests.

Appendix 1 – National Policy versus Cyber Deterrence

Policy Document \ Policy Needs	Attribution	Penalty	Credibility	Definition of Attack	Dependency	Counter Productivity	Awareness	Futility
National Security Strategy[1]	X	X	X	X	X		X	X
Executive Order 13231[2]							X	
National Strategy for Homeland Security[3]		X	X				X	X
Cyberspace Policy Review[4]		X					X	X
Comprehensive National Cyber Security Initiative[5]		X					X	
Homeland Security Presidential Directive 7[6]							X	
National Strategy for the Physical Protection of CI and Key Assets[7]							X	X

National Policy Shortfalls Tool

[1] U.S. President, *National Security Strategy*, (Washington, DC: Government Printing Office, May 2010).

[2] U.S. President, *Executive Order 13231 – Critical Information Protection in Information Age*, (Washington, DC: Government Printing Office, October 16, 2001).

[3] U.S. President, *National Strategy for Homeland Security*, (Washington, DC: Government Printing Office, July 16, 2002).

[4] U.S. President, *Cyberspace Policy Review*, (Washington, DC: Government Printing Office, 2009).

[5] U.S. President, *The Comprehensive National Cybersecurity Initiative*, (Washington, DC: Government Printing Office, January 7, 2011).

[6] U.S. President, *Homeland Security Presidential Directive 7*, (Washington, DC: Government Printing Office, December 17, 2003).

[7] U.S. President, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, DC: Government Printing Office, February 2003).

Policy Document \ Policy Needs	Attribution	Penalty	Credibility	Definition of Attack	Dependency	Counter Productivity	Awareness	Futility
National Military Strategy[8]							X	X
Strategy for Homeland Defense and Civil Support[9]							X	X
DoD Policy and Responsibilities for Critical Infrastructure Directive[10]							X	
Defense Industrial Base: CI and Key Resources Sector Specific Plan[11]							X	X
Department of Defense Strategy for Operating in Cyberspace[12]		X	X	X			X	
National Strategy to Secure Cyber Space[13]	X	X	X				X	
National Infrastructure Protection Plan[14]			X				X	X

National Policy Shortfalls Tool

[8] Chariman Joint Chiefs of Staff. *National Military Strategy*, (Washington DC: Government Printing Office, February 8, 2011).

[9] U.S. Department of Defense, *Strategy for Homeland Defense and Civil Support*, (Washington DC: Department of Defense June 30, 2005).

[10] U.S. Department of Defense, *DoD Policy and Responsibilities for Critical Infrastructure*, (Washington DC: Department of Defense, January 14, 2010).

[11] U.S. Department of Defense, *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan*, (Washington DC: Department of Defense, May 2007).

[12] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (Washington DC: Department of Defense, July 2011).

[13] U.S. Department of Homeland Security. *National Strategy to Secure Cyberspace*, (Washington, DC: Department of Homeland Security, 2003).

[14] U.S. Department of Homeland Security. *National Infrastructure Protection Plan*, (Washington, DC: Department of Homeland Security, 2009).

BIBLIOGRAPHY

111th Cong., 1st sess. *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance.* Washington DC: Government Printing Office, 2009.

112th Cong., 1st sess. *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology.* Washington, DC: Government Printing Office, 2011.

Anderson, Nate. "Massive DDoS attacks target Estonia; Russia accused." http://arstechnica.com/security/news/2007/05/massive-ddos-attacks-target-estonia-russia-accused.ars (accessed October 16, 2011).

Baker, Ralph O. "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations." Military Review (May-June 2006): 13-32.

Baker, Stewart. "In The Crossfire: Critical Infrastructure in the Age of Cyber War." http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf (accessed October 15, 2011).

---. "In the Dark: Crucial Industries Confront Cyberattacks." http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf (accessed October 15, 2011).

Barabasi, A. *Linked: The New Science of Networks.* New York: Basic Books, 2002.

Barnett, R. W. *Information Operations, Deterrence, and the Use of Force.* Newport: Naval War College, 1998.

British Broadcasting Corporation. "Estonia fines man for 'cyber war'." http://news.bbc.co.uk/2/hi/technology/7208511.stm (accessed November 11, 2011).

---. "Iran says nuclear programme was hit by sabotage." http://www.bbc.co.uk/news/world-middle-east-11868596 (accessed November 13, 2011).

Bunn, M. Elaine. "Can Deterrence Be Tailored?" Strategic Forum, 255, (June 2007): 1-8.

Byers, Eric, Andrew Ginter, and Joel Langill. "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems." White Paper, Tofino Security, 2011.

Certoff, M. "Cyber ShockWave exposed missing links in US security." http://fcw.com/articles/2010/03/11/commentary-chertoff-cyber-shockwave.aspx (accessed October 5, 2011).

Chariman Joint Chiefs of Staff. *National Military Strategy.* Washington DC: Government Printing Office, February 8, 2011.

Clarke, Richard A. *Cyberwar.* New York: HarperCollins, 2010.

Clausewitz, Carl Von. *On War.* New York: Alfred A. Knopf, 1993.

Coleman, Kevin G. *Cyber Commander's Handbook: The Weaponry & Strategies of Digital Conflict.* McMurray: Technolytics, 2009.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (accessed February 25, 2012).

de Armond, Paul. "Netwar in the Emerald City: WTO Protest Strategy and Tactics," in Networks and Netwars: The Future of Terror, Crime, and Militancy, 201-235. Edited by John Arquilla, & David Ronfeldt. Santa Monica: RAND, 2001.

DeNileon, Gay Porter. "Critical Infrastructure Protection: The Who, What, Why, and How of Counterterrorism Issues." 2008. http://www.mrws.org/Terror/Counterterrorism.htm (accessed October 15, 2011).

Denning, Dorthy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in Networks and Netwars: The Future of Terror, Crime, and Militancy, 239-288. Edited by John Arquilla, & David F. Ronfeldt. Santa Monica: RAND, 2001.

Durr, Charles W. "Nuclear Deterrence in the Third Millennium." Thesis, Carlisle Barracks: U.S. Army War College, 2002.

Flynn, S. *The Edge of Disaster.* New York: Random House, 2007.

Gaddis, John Lewis. *Strategies of Containment: A Critical Appraisal of Postwar American National Security.* New York: Oxford University Press, 1982.

Greenemeier, Larry. "Estonian 'Cyber Riot' Was Planned, But Mastermind Still A Mystery." Information Week. http://www.informationweek.com/news/201202784 (accessed January 6, 2012).

Hafner, K., and J. Markoff. *Cyber Punk: Outlaws and Hackers on the Computer Frontier.* New York: Simon and Schuster, 1991.

Hayes, Richard E., and Gary Wheatley. *Information Warfare and Deterrence.* Washington, DC: National Defense University, 1996.

Hoffman, Bruce. *The Use of the Internet by Islamic Extremists.* Santa Monica: RAND, 2006.

Jackson, Patrick. “The cyber raiders hitting Estonia.” British Broascasting Corporation. http://news.bbc.co.uk/2/hi/europe/6665195.stm (accessed February 25, 2012).

Kahn, H. *On Thermonuclear War.* Princeton: Princeton University Press, 1961.

Kaufmann, William. *The Evolution of Deterrence 1945–1958.* Pittsburgh: RAND, 1958.

Kelly, Spencer. “BBC team exposes cyber crime risk.” British Broadcasting Company. http://news.bbc.co.uk/2/hi/programmes/click_online/7932816.stm (accessed October 15, 2011).

Kitson, Frank. *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping.* New York: Stackpole, 1971.

Kraakman, Reinier H. “Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy.” *Journal of Law, Economics, & Organization,* Vol. 2, No. 1 (Spring 1986): 53-104.

Kramer, Franklin D. *Cyber Power and National Security: Policy Recommendations for a Strategic Framework.* Washington, DC: National Defense University, 2009.

Langner, Ralph. *Cracking Stuxnet, a 21st-century cyber weapon.* Long Beach, February 2011.

Libiciki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica: RAND, 2009.

Long, A. Deterrence: *From Cold War to Long War.* Santa Monica: RAND, 2008.

Markoff, John. “Before the gunfire, cyberattacks.” New York Times. http://www.nytimes.com/2008/08/13/technology/13iht-13cyber.15227999.html (accessed January 3, 2012).

Marks, Paul. “Pentagon readies its cyberwar defences.” New Scientist. http://www.newscientist.com/article/mg20126994.600-pentagon-readies-itscyberwar-defences.html (accessed October 12, 2011).

McCallie, Donald, Jonathan Butts, and Robert Mills. “Security analysis of the ADS-B implementation in the next generation air transportation system.” *International Journal of Critical Infrastructure Protection* (2011): 78-87.

McDonnell, Steve. *Code Complete,* Redmond: Microsoft Press, 2004

McGuinn, Martin G. “Prioritizing Cyber Vulnerabilities.” Washington, DC: National Infrastructure Advisory Council, 2004.

Melman, Yossi. “Computer virus in Iran actually targeted larger nuclear facility.” Haaretz.com. http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052 (accessed November 11, 2011).

Melshen, Paul. “Mapping Out a Counterinsurgency Campaign Plan: Critical Considerations in Counterinsurgency Campaigning.” Small War and Insurgencies 18, no. 4 (December 2007): 665-698.

Meserve, Jeanne. “Sources: Staged cyber attack reveals vulnerability in power grid.” Cable News Network. http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US (accessed October 15, 2011).

Messmer, Ellen. “U.S. cyber counterattack: Bomb 'em one way or the other.” Network World. http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html (accessed September 24, 2007).

Moran, Ned. “Achieving Cyber Deterrence.” April 24, 2009. The Cuckoo’s Egg. http://gucosc011.blogspot.com/2009/04/achieving-cyber-deterrence.html (accessed February 26, 2012).

Njolstad, Olav. “The Development and Proliferation of Nuclear Weapons.” Nobel Prize. http://www.nobelprize.org/educational/peace/nuclear_weapons/readmore.html (accessed October 15, 2011).

Oleg, Kupreev, and Ulasen Sergey. *Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review.* Technical Paper, Minsk: VirusBlokAda, 2010.

Perez, Juan Carlos. “DDoS Attackers Continue Hitting Twitter, Facebook, Google.” PC World. http://www.pcworld.com/businesscenter/article/169893/ddos_attackers_continue_hitting_twitter_facebook_google.html (accessed October 13, 2011).

Lewis, James. “Securing Cyberspace for the 44th Presidency.” Washington, DC: Center for Strategic and International Studies, 2008.

Robb, Bev. “Guest Article: The Evolution of Cyber Crime.” Roer. http://www.roer.com/node/652 (accessed September 27, 2011).

Sellers, Peter. *Dr. Strangelove Or: How i Learned to Stop Worrying and Love the Bomb*. DVD. Directed by Stanley Kubrick. Los Angles: Turner Classic Movies, 1964

Silva, Veronica C. “Critical infrastructure sectors prone to cyber security threats.” MIS Asia. http://mis-asia.com/resource/security/critical-infrastructure-sectors-prone-to-cyber-security-threats--study/ (accessed October 12, 2011).

Sofaer, Abraham D., and Seymour E. Goodman. *The Transnational Dimension of Cyber Crime and Terrorism.* Stanford: Hoover Institution Press, 2001.

Statistics Estonia. “EU Statistics.” http://www.stat.ee/international-statistics. (February 2012).

Taipale, K. A. “Cyber-Deterrence, in Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization,” Edited by Pauline C. Reich. Hershey: IGI Global, 2009.

Talbot, David. “Cybercrime Needs to be Top Priority, Says Obama Aide.” Technology Review. http://www.technologyreview.com/computing/25074/ (accessed October 15, 2011).

---. “Exposing Hackers as a Deterrent.” Technology Review. http://www.technologyreview.com/computing/25060/page1/ (accessed October 15, 2011).

The Economist. “Estonia and Russia: A Cyber-Riot.” http://www.economist.com/node/9163598 (accessed February 8, 2012).

TrendMicro. “Stuxnet Malware Targeting SCADA Systems.” TrendMicro. http://threatinfo.trendmicro.com/vinfo/web_attacks/Stuxnet%20Malware%20Targeting%20SCADA%20Systems.html (accessed November 13, 2011).

U.S. Department of Defense. *Defense and Civil Support Strategy for Homeland.* Washington DC: Department of Defense June 30, 2005.

---. *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan.* Washington DC: Department of Defense, May 2007.

---. *Department of Defense Strategy for Operating in Cyberspace.* Washington DC: Department of Defense, July 2011.

---. *Deterrence Operations Joint Operating Concept - Version 2.0.* Washington DC: Department of Defense, 2006.

---. *DoD Policy and Responsibilities for Critical Infrastructure.* Washington DC: Department of Defense, January 14, 2010.

---. *National Defense Strategy.* Washington DC: Department of Defense, June 2008.

U.S. Department of Homeland Security. *National Infrastructure Protection Plan.* Washington, DC, 2009.

---. *National Strategy to Secure Cyberspace.* Washington, DC, 2003.

U.S. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02. Washington, DC: Joint Chiefs of Staff, November 8, 2010.

U.S. President. *Cyberspace Policy Review.* Washington, DC: Government Printing Office, 2009.

---. *Executive Order 13231 – Critical Information Protection in Information Age.* Washington, DC: Government Printing Office, October 16, 2001.

---. *Homeland Security Presidential Directive 7.* Washington, DC: Government Printing Office, December 17, 2003.

---. *National Strategy for Homeland Security*. Washington, DC: Government Printing Office, July 16, 2002.

---. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington, DC: Government Printing Office, February 2003.

---. *National Security Strategy*. Washington, DC: Government Printing Office, May 2010.

---. *The Comprehensive National Cybersecurity Initiative.* Washington, DC: Government Printing Office, January 7, 2011.

---. *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63.* Washington, DC: Government Printing Office, 1998.

Wheeler, David A. *Techniques for Cyber Attack Attribution.* Alexandria: Institute for Defense Analysis, 2003.

Wildstrom, Stephen. "Why Is the Government Vulnerable to a Simple Cyber Attack?" Business Week. http://www.businessweek.com/the_thread/techbeat/archives/2009/07/why_is_the_gove.html (accessed October 10, 2011).

Wilshusen, Gregory C. "CYBERSECURITY: Challenges in Securing the Modernized Electricity Grid," U.S. Government Accountability Office, February 28, 2012.

VITA

Most recently, LCDR Rivera completed a tour as the Combat Systems Officer aboard USS TUCSON (SSN 770). As the Combat Systems Officer he was responsible for the weapons and sonar systems, and force protection. As Officer of the Deck he was also responsible for the training and development of his watch section.

LCDR Rivera initially enlisted in the Marine Corps in 1993 and was subsequently commissioned in 2000 from Officer Candidate School, Pensacola, Florida. Following initial training LCDR Rivera served onboard the USS NEVADA (SSBN 733) and as an action officer on the EUCOM staff in the Joint Interagency Coordination Group. Lieutenant Commander Rivera is a graduate of Rensselaer Polytechnic Institute and has a degree B.S. in Computer Science.